Aki Karppinen

Palomuurin asennus ja käyttöönotto

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietoverkot

Insinöörityö

11.5.2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Aki Karppinen Palomuurin asennus ja käyttöönotto 50 sivua + 3 liitettä 11.5.2015
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja(t)	yliopettaja Janne Salonen yrityksen edustaja Arto Tuominen

Insinöörityön tavoitteena oli toteuttaa palomuurivaihto yrityksessä. Erilaisten palomuurivaihtoehtojen vertailussa päädyttiin Zyxelin Zywall 310:een. Vaihtoa varten tehdyssä työsuunnitelmassa työvaiheet esiteltiin ja aikataulutettiin.

Teoriaosuudessa esiteltiin palomuureihin ja työssä käytettäviin menetelmiin liittyviä ominaisuuksia, jotka tukivat käytännön toteutusta. Tärkeimpiä aihealueita olivat suodatusmenetelmät, osoitemuunnos ja VPN-yhteydet. Käytännön osiossa toteutettiin ja esiteltiin palomuuriasetukset.

Lopuksi toteutettiin vaihtotyö, johon liittyi palveluiden toiminnan tutkiminen ja korjaaminen. Palveluiden toimintaa tarkkailtiin palomuurilokista ja verkon laitteista. Tarkkailun avulla asetukset pystyttiin korjaamaan toimiviksi.

Lopputuloksena syntyi kokonaisuus, jossa palomuuri toimi keskeisenä osana verkkojen toteutusta ja niiden liikenteen rajoittamista. Palomuuri suodatti, antoi IP-osoitteet laitteille sekä yhdisti ne oikeisiin verkkoihin. Insinöörityön pohjalta yrityksessä pystyttiin dokumentoimaan järjestelmiä ja parantamaan yrityksen tietoturvasuunnitelmaa.

Avainsanat	Palomuuri, palomuurivaihto, suodatus, VPN, NAT, VLAN

Author(s) Title Number of Pages Date	Aki Karppinen The Firewall Installation and Implementation 50 pages + 3 appendices 11 May 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data networks
Instructor(s)	Janne Salonen, Principal Lecturer Arto Tuominen, Company representative

The aim of the thesis was to perform a firewall exchange in a company. Different firewalls were compared and Zyxel Zywall 110 was selected. A work schedule was made describing and detailing the work phases.

The theoretical part elaborates the properties of firewalls and the work methods used on in this study that contribute to the practical implementation. The most important topics are filtering methods, network translations and VPN connections. In the practical part the firewall settings were implemented and presented.

In the end the firewall exchange was implemented. It included the examination of the operation of the services. The operations of the services were monitored by the firewall log and the network devices. The monitoring allowed the fixing of the setting failures.

As an outcome of this thesis, the new firewall was implemented and it plays a crucial part in the operation of the network and the restriction of the network traffic. The firewall filters the network traffic and gives IP addresses to the network devices and connects them to the right networks. On the basis of this thesis the systems in the company could be documented and the information security plan improved.

Keywords	Firewall, firewall exchange, filtering, VPN, NAT, VLAN

Sisällys

Lyhenteet

AES	Advanced Encryption Standard. Lohkosalausmenetelmä.
AH	Authentication Header. Protokolla, jota käytetään IPSec:ssä pakettivirtojen turvaamiseen.
ARP	Address Resolution Protocol. Ethernet-verkossa käytettävä protokolla, jolla selvitetään IP-osoitteita vastaavat MAC-osoitteet.
BGP	Border Gateway Protocol. Reititysprotokolla.
CFI	Canonical Format Indicator. 802.1Q-standardin TCI-kentän ethernet-verkon yhteensopivuuden tutkimiseen käytetty kenttä.
DH2	Diffie-Hellman. Julkinen avaintenvaihto- ja tiedonsalausprotokolla 1024-bittisellä avaimella.
DHCP	Dynamic Host Configuration Protocol. Protokolla mm. IP-osoitteiden jakamiseen.
DMZ	Demilitarized Zone. Tarkoittaa yleensä fyysistä tai loogista aliverkkoa.
DNS	Domain Name System. Järjestelmä, jolla muutetaan IP-osoitteet verkkotunnuksiksi.
EAP	Extensible Authentication Protocol. Käyttäjätunnistusprotokolla.
ESP	Encapsulating Security Payload. Protokolla, jota käytetään IPSec:ssä pakettivirtojen turvaamiseen.
FSC	Frame Check Sequence. Ethernet-kehyksessä käytettävä virheenpaljastuskenttä.
FTP	File Transfer Protocol. Tiedostonsiirtoprotokolla.
HTTP	Hypertext Transfer Protocol. Tiedonsiirtoprotokolla.

HTTPS	Hypertext Transfer Protocol Secure. Salattu tiedonsiirtoprotokolla.
IETF	Internet Engineering Task Force. Internet-protokollien standardisoinnista vastaava organisaatio.
IKE	Internet Key Exchange. IPSec-protokollan kanssa käytettävä avainten-vaihtoprotokolla, joka koostuu ISAKMP, Oakleyin ja SKEME:n yhdistelmästä.
IP	Internet Protocol, TCP/IP-mallin verkkokerros.
IPv4	Internet Protocol version 4, TCP/IP-mallin protokolla, versio 4.
IPSec	Internet Protocol Security. Tietoturvaprotokollajoukko TCP/IP-mallin verkkokerroksessa.
ISAKMP	Internet Security And Key Management Protocol. Protokolla, joka varmistaa turva-assosiaatiot (SA) ja salausavaimet.
LAN	Local Area Network. Lähiverkko.
MAC	Media Access Control. Verkko-osoitteen yksilöivä osoite.
NAT	Network Address Translation. Osoitemuunnos.
NAT-T	Network Address Translation Traversal. Joukko menettelyjä, joilla pyritään turvaamaan IPSec:llä suojattujen IP-pakettien läpimeno osoitemuunnoksessa.
NATT	Network Address Translation Traversal. Tarkoittaa samaa kuin NAT-T.
OAKLEY	IKE:ssä käytettävä protokolla avainten hyväksymiseen ja vaihtoon käyttäen Diffie-Hellmanin avaintenvaihtoalgoritmia.
OSI	The Open Systems Interconnection. Tiedostonsiirtoprosessin kuvaus seitsemässä kerroksessa.

PAT	Port Address Translation. Porttimuunnos.
PFS	Perfect Forward Secrecy. Varmistaa avaintenvaihdon turvallisuuden.
PING	Yksinkertainen TCP/IP-mallin työkalu, jolla voi testata laitteiden saavutettavuutta.
PRB	Policy-Based routing. Palomuuripolitiikka, jolla reititetään liikennettä.
SA	Security Association. Sopimus, joka määrittää tietyn menetelmän esimerkiksi VPN-yhteyksien suojaukseen.
SHA	Secure Hash Algorithm. Liikenteen salauksessa käytetty tiiviste, joka sekoittaa viestin.
SKEME	Secure Key Exchange Mechanism. Avaintenvaihtoprotokolla, joka kuuluu osaksi IKE:ä.
SPI	Stateful Packet Inspection. Tilallinen pakettisuodatus, jossa pidetään kirjaa yhteyksistä.
SSH	Secure Shell. Protokolla, jolla voidaan luoda pääteyhteyksiä tai suojata muuta liikennettä.
SSL	Secure Sockets Layer. Erillinen suojattu taso esimerkiksi www-sivujen lukemiseen tai tiedonsiirtoon.
Telnet	Telnet-protokollaa käyttävä yhteys esimerkiksi asiakaslaitteen ja verkkolaitteen välillä liikennöimseen.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla yhteyden luomiseen verkkolaitteiden välille.
TCP/IP	Transmission Control Protocol / Internet Protocol. Internetliikennöinnissä käytettävien tiedostonsiirtoprotokollien yhdistelmä.

UDP	User Datagram Protocol. Tietoliikenneprotokolla, jolla mahdollistetaan tietojen siirto.
VLAN	Virtual Local Area Network. Virtuaalilähiverkko.
VPN	Virtual Private Network. Näennäinen yksityisverkon muodostustapa.
WAN	Wide Area Network. Laajaverkko.
Web	Yleisesti käytetty lyhenne sanalle WWW (Word Wide Web)
WLAN	Wireless Local Area Network. Langaton lähiverkko.

1 Johdanto

Tietoliikenne on kehittynyt valtavasti 1980-luvulta asti ja jatkaa kasvuaan edelleen. Nykyään liikenteen kasvu perustuu mobiiliympäristöihin ja langattomiin verkkoihin.. Älypuhelimet ja muut kannettavat laitteet lisääntyvät, ja niiden ohjelmat toimivat internetissä taukoamatta.

Tietoliikenteen määrä ja sen kasvaminen vaikuttavat oleellisesti myös verkon laitteiden toimintaan. Erilaiset laitteet, käyttöjärjestelmät, virukset ja hyökkäystavat lisääntyvät ja monipuolistuvat ja siksi täytyy kehittää uusia ratkaisuja hyökkäyksien estämiseksi. Kasvavat tietoturvaongelmat ovat tuoneet markkinoille myös uusia tietoturvaa parantavia tuotteita. Nykyään esimerkiksi kuluttajapuolen modeemeissa saattaa olla sisäänrakennettuna palomuuri.

Insinöörityön aihe syntyi, kun eräässä yrityksessä tuli tarve kartoittaa ja uusia palomuuri, jotta palveluiden toiminta pystyttäisiin turvaamaan. Opinnäytetyö käsittelee palomuurin asetuksien laittamista ja itse asennusta. Käytännön osiossa käydään läpi työn kannalta tärkeimpiä ominaisuuksia sekä tarkastellaan nykyistä turvatasoa. Palomuuriasetukset saadaan dokumentoitua opinnäytetyön pohjalta.

Opinnäytetyön tilaajana on Fixcom Oy, joka on pieni pääkaupunkiseudulla toimiva IT-yritys. Yritys toimii pääkaupunkiseudulla tarjoten palveluita virtuaalipalvelimista sähköpostipalveluihin sekä tietoverkkojen suunnitteluun ja asennukseen. Käytännön testaustaukset ja vaihtotyö toteutettiin yrityksen tiloissa. Opinnäytetyössä alkuperäiset IP-osoitteet ja tarkat asetukset on muutettu tietoturvasyistä.

2 Palomuuri yritysverkon suojana

Nykyään yritykset kohtaavat erilaisia haasteita suunnitellessaan tietoturvakäytäntöjä ja estääkseen mahdolliset uhkatekijät. Enää ei riitä se, että tietokoneissa on sovelluspalomuurit ja virustorjunta, vaan mahdolliset uhkatekijät olisi hyvä estää jo ennen sisäverkkoon pääsyä. Koska täysin turvallista järjestelmää tai palomuuria ei pystytä tekemään, on tärkeää panostaa rakenteelliseen tietoturvaan. Useilla verkkolaitteilla rajoite-

taan ja suodatetaan verkkoliikennettä eri osa-alueilla. Yhden osan vuotaminen ei näin aiheuta koko järjestelmän kaatumista.

Palomuuri-termi on mainittu ensimmäisiä kertoja jo 1960-luvulla, josta se on säilynyt muuttumattomana tähän päivään asti. Palomuureja on kehitetty aktiivisesti 1980-luvulta lähtien. Kehitystä on vauhdittanut 1980-luvun lopulla löydetty ensimmäinen mato nimeltä Morris [1].

Nykyisin internetiin kytketään suuret määrät erilaisia laitteita, joita täytyy suojella erilaisin toimenpitein. Palomuurit ovat olleet osana tätä suojausta ja niitä on integroitu käyttöjärjestelmiin. Ensimmäinen Windowsin ohjelmallinen palomuuri tuli Windows XP Service Pack 2:n mukana. Sen jälkeen se on löytynyt jokaisesta Windows-versiosta [2]. Mac-tietokoneista se löytyy versiosta 10.5.1 eteenpäin [3].

Palomuuri on laite, joka suojaa suoria yhteyksiä sisäisen ja ulkoisen verkon välillä. Se estää mahdolliset tunkeilijat ja päästää lävitseen toivotun liikenteen. Sen toiminta perustuu sääntöihin, jotka määritellään yksityiskohtaisesti. Säännöt tulisi pohjautua tietoturvakäytäntöihin tai ainakin johonkin dokumentaatioon. Dokumentoinnin avulla verkon toimintaa on helpompi ymmärtää ja mahdolliset virheasetukset saadaan helpommin korjattua. Verkon ylläpitäminen on helpompaa, kun se on dokumentoitu ainakin jollakin tasolla.

Palomuureja on kahdenlaisia – sovellus- ja rautapalomuureja. Sovellusmuurit nimensä mukaisesti toimivat OSI-mallin sovelluskerroksella. Sovelluspalomuurilla pystytään hyväksymään ohjelmatasolla, mitkä tietokoneen ohjelmat saavat liikennöidä ja mihin suuntaan. Liikennettä voisi olla esimerkiksi ohjelman yhdistäminen ulkoverkossa olevaan palvelimeen tai sisäverkossa toiseen laitteeseen. Toisin kuin rautapalomuurin kanssa, toiminta voi olla hyvinkin näkyvää käyttäjälle.

Internetissä olevia työasemia ja laitteita on nykyään paljon, koska erilaiset mobiililaajakaista ja kännykkäverkon jakaminen mahdollistavat nopean internetyhteyden missä vain. Laitteet ovat suoraan internetissä, joten sovelluspalomuurin pitäisi olla asennettuna ja päällä joka laitteessa. Tietokoneissa voi olla itsenäisiä ohjelmia, jotka voivat salata tai ottaa yhteyksiä suoraan internetiin, joten niiden liikennettä ei välttämättä pystytä

tarkkailemaan rautapalomuurilla. Silloin sovelluspalomuuri on oivallinen väline oman tietokoneen yhteyksien sallimiseen ja tarkkailuun.

Rautapalomuurit ovat erillisiä laitteita, jotka asennetaan julkisen ja sisäisen verkon väliin. Se voi olla esimerkiksi reitittimen tai modeemin takana. Palomuureja voidaan käyttää myös verkon muissa osissa, mutta väärin asennettuna ne voivat haitata tai estää verkon liikennettä.

Toisin kuin sovelluspalomuuri, rautapalomuurit toimivat OSI-mallin alemmilla kerroksilla. Tarkoituksena on tarkkailla liikennettä IP-tasolla, tehdä pääsynhallintaa ja pakettisuodatusta. Yhteyksissä voidaan käyttää käyttäjätunnistusta, joka lisää tietoturvaa.

Palomuuri ei ole ainut laite, joka suojaa yritystä uhkilta, mutta se pitää mieltää osaksi yrityksen tietoturvaa. Se toimii tehokkaasti reitittimien, kytkimien ja muiden verkkolaitteiden kanssa. Siihen laitetaan sellaiset asetukset, että yrityksen toiminta ei rajoitu verkon käytön osalta. Ominaisuusiltaan ja tehokkuudeltaan sen tulisi vastata helposti yrityksen tarpeita. Ominaisuudet ja tehokkuus tulee ottaa huomioon verkon suunnittelussa ja tietoturvakäytäntöä luotaessa. Palomuuria valittaessa pitää ottaa huomioon esimerkiksi VPN-yhteyksien määrä, verkon nopeus, salaustavat ja verkkoliikenteen palvelut sekä niiden kuormittavuus. Jos tietoverkko suojattaisiin alimitoitetulla laitteella, joka ei suoriutuisi perustehtävistä riittävässä ajassa, se voisi pahimmillaan lamauttaa verkkoliikenteen kokonaan.

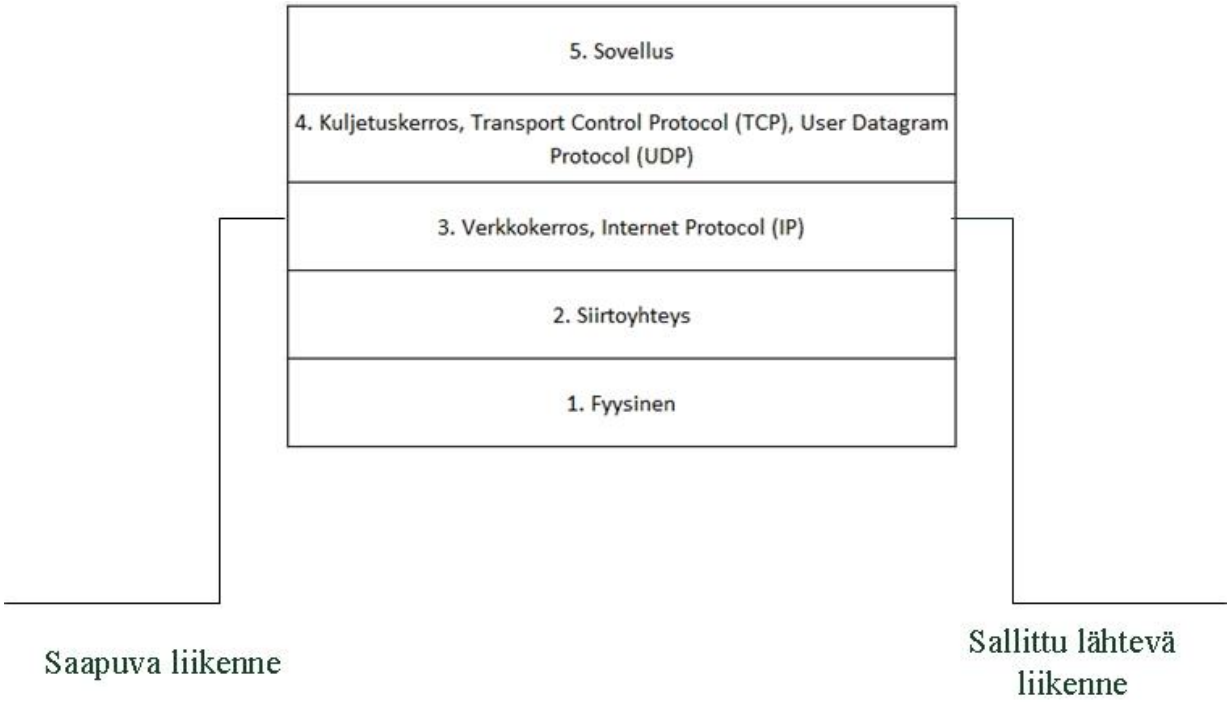
2.1 Suodatusmenetelmät

Palomuureissa on erilaisia suodatusmenetelmiä, joilla tulevaa liikennettä pyritään tutkimaan ja erottelemaan. Tarkoituksena on estää asiaton liikenne suoraan verkkoon tai palveluun. Suodatusmenetelmät voidaan jakaa kolmeen ryhmään: pakettisuodattimiin, välityspalvelimiin ja sovellustason yhdyskäytäviin. [4, s. 187.]

2.1.1 Tilaton pakettisuodatus

Tilaton pakettisuodatus on käytäntö, jota kutsutaan pääsylistaksi (ACL). Tämän englanninkielisiä lyhenteitä ovat Access List tai Access Control List. Pääsylistoihin on kir-

jattu tietyt asetukset, joiden puitteissa IP-paketit hyväksytään tai hylätään. Kun IP-paketti suodatetaan, tarkistetaan pääsylistojen mukaan, voidaanko paketti lähettää eteenpäin vai poistetaanko se. Suodatus toimii OSI-mallin kolmannessa kerroksessa [5, s. 89.]. Tilattomalla suodatuksella jokainen yhteys tarkistetaan uudelleen säännöstöistä. Kuvassa 1 on esitetty tilattoman pakettisuodatuksen idea.



Kuva 1. Yksinkertainen pakettisuodatus OSI-mallin 3. kerroksessa. [6, s. 89.]

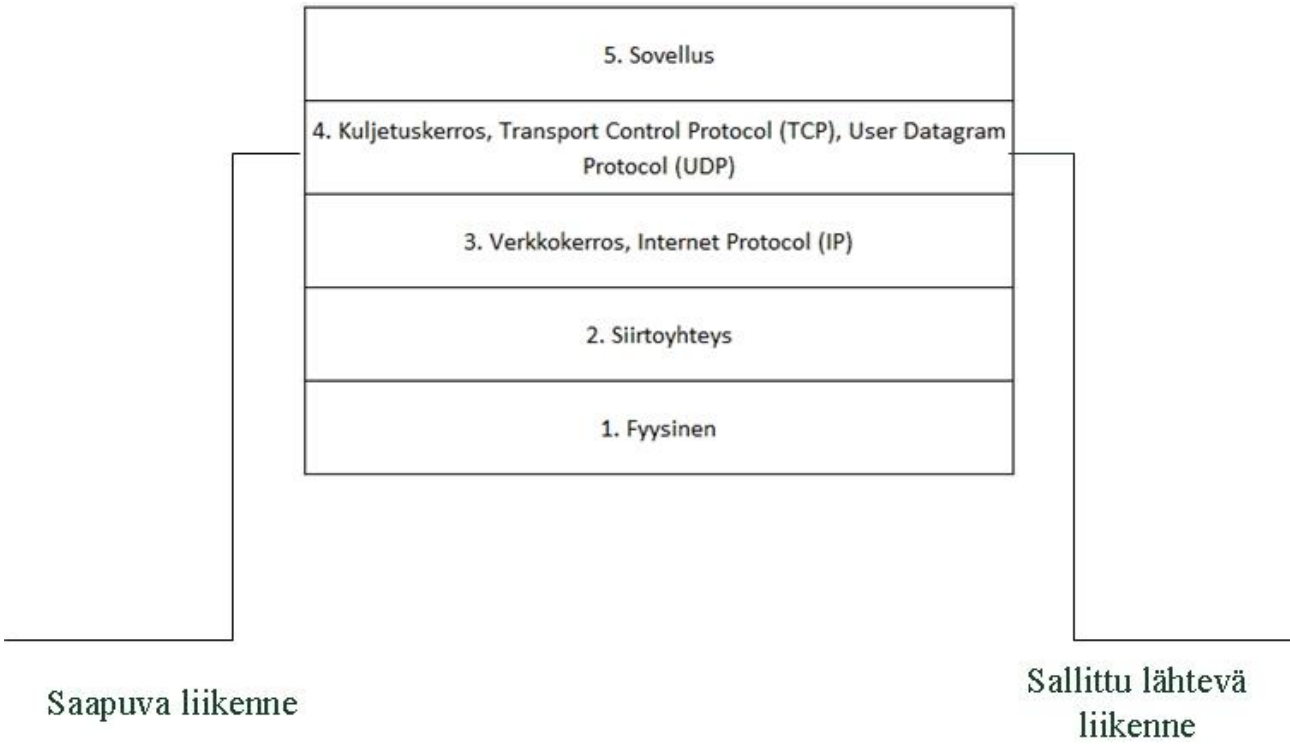
Thomasin esittämässä mallissa (kuva 1) saapuva IP-paketti käy läpi tasot fyysisestä verkkokerrokseen. Kun suodatus on tehty, paketti siirretään eteenpäin käänteisessä järjestyksessä verkkokerroksesta fyysiseen.

2.1.2 Tilallinen pakettisuodatus

Tilallinen pakettisuodatus, jota kutsutaan myös nimellä yhteyssuodatus (Stateful Packet Inspection, SPI), toimii TCP/IP-mallin neljännessä kerroksessa. Menetelmällä voidaan tutkia IP-paketin koko, lähettäjän ja vastaanottajan IP-osoitteet, portit ja niiden protokollat sekä asetetut liput. [7, s. 97.]

Yhteyssuodatuksessa avoimet ja jo suljetut yhteydet lisätään taulukkoon, jossa näkyy kaikki yhteyden tiedot. Näitä tietoja käytetään hyväksi, kun saman yhteyden paketteja tulee, jotta ne voidaan helpommin suodattaa ja lähettää eteenpäin. Jos yhteys on jo avoinna, siihen kuuluvat paketit on tärkeä saada hyväksyttyä ja lähettyä eteenpäin. Yhteyden tila nähdään TCP-järjestysnumerosta, joka löytyy myös taulukosta. [8, s. 98.]

Kun tulevat yhteydet pystytään rajaamaan tarkasti, tietoturva paranee huomattavasti. Käyttöönotto voi tuottaa hieman enemmän työtä, mutta se kannattaa, koska silloin liikennettä voidaan tutkia ja suodattaa mahdolliset hyökkäysyritykset. Esimerkkinä voitaisiin sallia vain http-yhteydet toimistoverkosta, jolloin sallitaan toimistoverkon IP-osoitteiden yhteydet http-protokollalla porttiin 80. Minkään muun protokollan tai IP-osoitealueen ei pitäisi päästä sen jälkeen läpi. Verkko- ja kuljetuskerroksella tehtävät suodatukset eivät estä esimerkiksi ylemmille kerroksille paketoidun haitallisen koodin etenemistä.



Kuva 2. Yhteydellisessä pakettisuodatuksessa tarkastetaan IP-paketin portit. [9, s. 96.]

Tilallisessa pakettisuodatuksessa yhteys käy läpi tasot fyysisestä kuljetuskerrokseen. Thomasin mallissa sallittu paketti jatkaa eteenpäin käänteisessä järjestyksessä (kuva 2).

2.1.3 Sovellustason yhdyskäytävä

Sovellusyhdyskäytävää kutsutaan usein Proxy-palvelimeksi. Se toimii yleensä julkisen ja sisäisen verkon rajapinnassa, jossa tulevat yhteydet tarkistetaan ja suodatetaan ennen kuin ne ehtivät sisäverkkoon.

Tämänkaltaisen palomuurin käyttämisessä on monenlaisia etuja. Sen avulla tulevat paketit voidaan tutkia TCP/IP-mallin alempien kerrosten lisäksi myös sovelluskerroksessa. Sovelluskerroksessa tieto pystytään purkamaan kokonaisuudessaan, jolloin sen kaikkea tietoa voidaan tutkia ja sen avulla tehdä päätös, lähetetäänkö IP-paketti eteenpäin. [10.]

Sovellustason käyttämisen etuja ovat käyttäjätunnistus ja salaus. Liikennettä voidaan rajoittaa käyttöoikeuksilla ja tiedon salaukseen voidaan käyttää salausalgoritmeja. Nämä ovatkin tärkeitä elementtejä nykyisessä tiedonsiirrossa, jossa tieto halutaan pitää vain niiden henkilöiden saatavilla, joille se kuuluu sekä varmistaa tiedon muuttumattomuus.

Välityspalvelin vertailee tulevia IP-paketteja omiin säännöstöihinsä ja tekee siltä pohjalta päätöksen, lähetetäänkö paketti eteenpäin. Jos paketti päätetään lähettää, Proxy-palvelin avaa tätä varten uuden yhteyden tämän ja vastaanottavan laitteen välille. [11, s. 105.] Vastaanottaja ei näe alkuperäistä lähettäjää, joten se lisää tietoturvaa, kun niin sanottuja suoria yhteyksiä ei ole.

2.2 Osoitemuunnos

Osoitemuunnos eli Network Address Translation (NAT) luotiin aikoinaan vähenevien IPv4-osoitteiden takia. Huomattiin, että kaikille verkkolaitteille ei tulevaisuudessa riitä omaa julkista IP:tä. NAT:n avulla pystytään käyttämään yhtä julkista IP-osoitetta use-

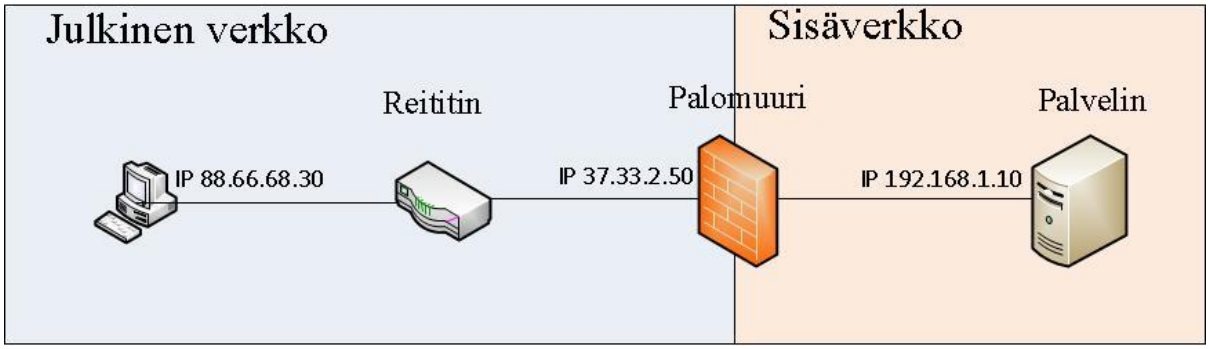
ammalle laitteelle, joille halutaan saada pääsy internetiin. [12, s. 100.] Ominaisuus soveltuu myös muihin tarkoituksiin.

NAT on nykyään hyvin yleinen ratkaisu ja siitä käytetään monenlaista nimitystä eri laitevalmistajien kesken. Kirjo on laaja, mutta kun tuntee käyttötarkoituksen, ei termeillä kään ole niin väliä. Seuraavassa on kuvattu muutamia tilanteita, jossa osoitemuunnos tehdään. Käsittelen myös tähän liittyen yleisimpiä termejä.

2.2.1 Staattinen NAT

Kuvassa 3 on kuvattu tilanne, jossa sisäverkon palvelimeen otetaan yhteyttä internetistä päin. Internetissä liikennöidään julkisella IP-osoitteella 37.33.2.50, joka saa NAT-osoitemuunnoksen jälkeen 192.168.1.10-kohdeosoitteen. Tätä kutsutaan staattiseksi osoitemuunnokseksi, jossa tietty julkinen IP-osoite muutetaan aina samaksi sisäverkon osoitteeksi [13, s. 102].

Protokollaportit muutetaan samalla tyylillä. Esimerkiksi sisäverkossa liikennöidään http-protokollalla porttiin 80, jonka palomuuri muuntaa osoitemuunnoksen yhteydessä porttiin 8080. Palvelimen näkökulmasta yhteys muodostetaan palomuurin kanssa eikä se tiedä julkisessa verkossa liikennöivästä työasemasta mitään. Esimerkiksi tässä opinnäytetyössä tehdään staattinen osoitemuunnos sähköpostipalvelimelle.



Kuva 3. Esimerkki staattisesta osoitemuunnoksesta.

Taulukko 1. Kuvan 3 esimerkin lähde- ja kohdeosoitteet.

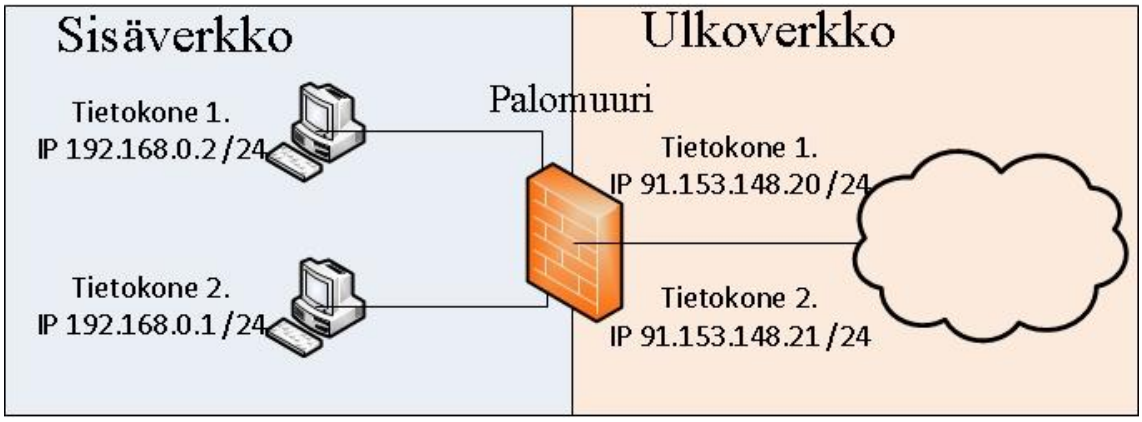
Julkinen verkko		Sisäverkko	
Lähdeosoite	**Kohdeosoite**	**Lähdeosoite**	**Kohdeosoite**
88.66.68.30	37.33.2.50	37.33.2.50	192.168.1.10

2.2.2 Dynaaminen NAT

Dynaaminen osoitemuunnos eroaa staattisesta siten, että sille on kerrottu IP-osoitealueet, joista se voi jakaa sisäverkon ja julkisen verkon IP-osoitteet ja muodostaa niistä parit. Sisäverkossa oleva laite saa yleensä ensimmäisen vapaana olevan osoitteen, jolla se pystyy liikennöimään internetiin päin. Esimerkiksi sisäverkossa on kaksi isäntäkonetta, joiden IP-osoitteet ovat 192.168.0.1 ja 192.168.0.2. Osoitealue on 192.168.0-1 – 192.168.0.5. Taulukon 2 esimerkin mukaan nämä IP-osoitteet saisivat 91.153.148.20- ja 91.153.148.21 -osoitteet. Jokaista yksityistä osoitetta varten on yksi julkinen osoite. Huomioitavaa tässä on se, että jos on käytössä vain yksi julkinen IP-osoite tai osoiteavaruudesta loppuvat julkiset osoitteet, laite tai laitteet eivät voi liikennöidä internetiin päin [14, s. 102].

Taulukko 2. Dynaamisen NAT-esimerkin sisäiset ja julkiset IP-osoitteet

	Sisäiset IP-osoitteet	Julkiset IP-osoitteet
Tietokone 1.	192.168.0.1	91.153.148.20
Tietokone 2.	192.168.0.2	91.153.148.21



Kuva 4. Taulukon 2 pohjalta tehty Dynaaminen NAT -esimerkkipiirros.

2.2.3 Porttimuunnos

Porttimuunnos eli Port Address Translation (PAT) tai toiselta nimeltään NAT Overloading on menetelmä, jolla yksityisen verkon IP-osoitteet muutetaan julkisen verkon IP-osoitteiksi. Tämä on kehitetty siksi, että useampi laite voisi liikennöidä internetiin yhden julkisen IP-osoitteen välityksellä.

Muutos toteutetaan samalla tavalla kuin aiemmin staattisen tai dynaamisen osoitemuunnoksen kohdalla, mutta tässä tapauksessa laitteiden liikenne tunnistetaan niiden ainutlaatuisten porttiosoitteiden mukaan. Osoitemuunnoksen tekemä laite pitää kirjaa tulleista yhteyksistä ja niiden IP-osoitteista ja porttinumerosta. Kun IP-paketti lähetään internetistä päin sisäverkon laitteelle takaisin, osoitemuunnos osaa ohjata liikenteen tähän tiettyyn IP-osoitteeseen.

Esimerkkinä porttiohjausmenetelmästä on kuvattu tietokoneen pyyntö Web-palvelimelle, jossa se haluaa avata tietyn internetsivun. Tietokone, jonka IP-osoite on 192.168.0.1, lähettää pyynnön julkiseen osoitteeseen 88.108.56.20 portilla 80. Tässä esimerkissä reititin tekee osoitemuunnoksen ja tallentaa tauluunsa liikennöivän tietokoneen tiedot. Tietokone käyttää lähdeporttina porttia 5000, joka osoitemuunnoksessa voidaan muuttaa esimerkiksi muotoon 5001. Kun paketti saavuttaa Web-palvelimen, sen lähdeosoite on reitittimen julkinen osoite portilla 5001. Kohdeosoite on web-palvelimen osoite 88.108.56.20 porttiin 80.

Web-palvelimen vastauksessa IP-paketti kulkee nyt käänteisessä järjestyksessä. Kohdeporttina käytetään liittymän julkista IP-osoitetta ja porttia 5001, josta yhteys tuli. Reititin katsoo osoitetaulustaan, mihin kohdeosoitteeseen osoitemuunnos tehdään ja muuttaa julkisen IP- ja porttiosoitteen sisäverkon vastaaviksi eli 192.168.0.1 porttiin 5000.

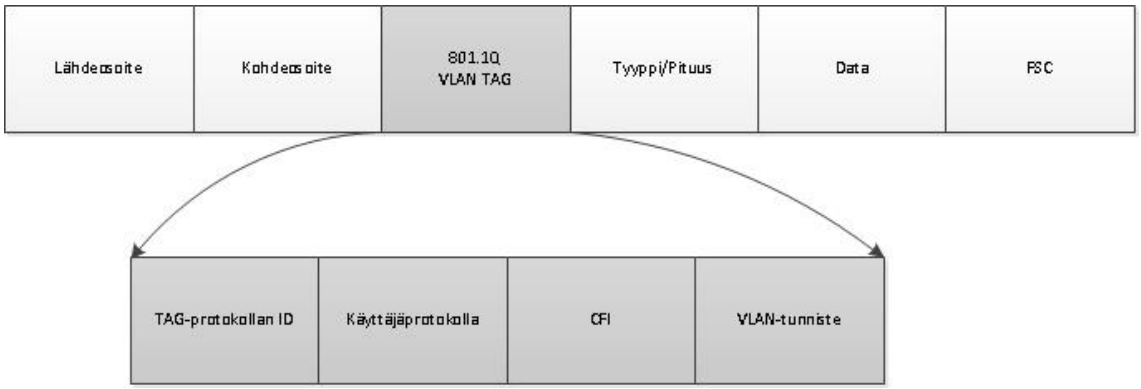
2.3 Virtuaalilähiverkko

Tietoverkkoja joudutaan ylläpitämään jatkuvasti ja välillä niihin on tehtävä muutoksia. Virtuaalilähiverkot (VLAN) tuovat tähän muutostyöhön helpotusta, sillä niitä käyttämällä fyysisiä muutoksia ei tarvitse tehdä. Verkon muutokset tapahtuvat kytkimien ja palomuurien hallinnasta. Virtuaaliverkkojen avulla pystytään myös parantamaan siirrettyjen tietojen luottamuksellisuutta [15, s. 227].

Virtuaaliverkko on yleislähetysalue (Broadcast domain), joka toimii samalla tavalla kuin paikallinen lähiverkko. Sen kautta mikä tahansa verkkolaite pystyy liikennöimään omalla alueellaan, joka on rajattu muista lähiverkoista. Muodostamalla tällaisia verkkoja voidaan koko verkon siirtokapasiteettia parantaa.

VLAN muodostuu normaalista Ethernet-kehyksestä, johon lisätään VLAN-merkintä (Vlan Tag). Erilaisia merkintätapoja on olemassa, mutta jos halutaan varmistaa laitteen toimivuus muiden laitteiden kanssa, täytyy käyttää 802.1Q-standardia [16, s. 235].

Kuvassa 5 näkyy VLAN 801.1Q -merkintä purettuna. Se sisältää ID-numeron, protokollan, CFI- ja VLAN-tunnisteen. CFI (Canonical Format Indicator) käytetään 802.1Q-standardin TCI-kentän Ethernet-verkon yhteensopivuuden tutkimiseen.



Kuva 5. VLAN-kehyksen rakenne [17].

Ciscolla on oma virtuaaliverkkojen muodostamistapansa, joka tunnetaan nimellä ISL (Inter-Switch Link). Kehyksen pituus voi olla maksimissaan 1548 tavua. Muut laitevalmistajat eivät tue ISL-menetelmää. [18.]

Virtuaalilähiverkkojen muodostamiseen on neljä tapaa:

- porttiperusteinen VLAN
- MAC-perusteinen VLAN
- verkkokerrosten palveluiden VLAN (OSI-mallin 3. kerros)

- policy-perusteinen VLAN. [19, s. 232.]

Porttiperusteisessa kytkimen portti tai portit pystytään liittämään tiettyyn virtuaalilähiverkkoon. Yksi portti voi kuulua ainoastaan yhteen verkkoon, mutta poikkeuksena on Trunk-portit, joihin voi kuulua useampi VLAN. [20. s. 231.]

Toinen samantyyppinen tapa on tehdä verkkoja MAC-osoitteen perusteella. Sen avulla voidaan niputtaa koneet niiden verkko-osoitteella tiettyyn VLAN-alueeseen [21, s. 231]. Vaikka laite siirrettäisiin eri paikkaan, kuuluisi se jo valmiiksi oikeaan VLAN:iin, mikä helpottaa laitteiden käyttöä.

VLAN:ja voidaan muodostaa myös verkkokerroksen avulla ja Policy-perusteisesti. Verkkokerroksella VLAN:ja voidaan hallinnoida esimerkiksi IP-osoitteen tai käyttäjätunnuksen mukaan [22]. Policy-perusteisessa pystytään laitteita ja käyttäjiä rajaamaan vielä tarkemmilla määrityksillä ja edellä mainittujen toteutustapojen yhteyskäytäntönä. Käytännön osuudessa VLAN:t määritellään tällä menetelmällä.

2.4 VPN-yhteydet

Nykyään tietoverkot mahdollistavat töiden tekemisen mistä vain erilaisten kiinteiden- ja mobiililiittymien kautta. Etätöitä tehdään yhä enemmän. Tämä vaatii tietoliikenteeltä ja laitteilta enemmän tietoturvan osalta. On varmistettava tiedon luottamuksellisuus, eheys ja käytettävyys [23].

Virtuaalinen lähiverkko (VPN) on tapa, jolla käyttäjän tietoverkko voidaan kytkeä osaksi yrityksen verkkoa turvallisesti [24, s. 236]. Käyttäjä tunnistautuu käyttäjätunnuksella ja salasanalla ja hänellä on sen jälkeen pääsy yrityksen resursseihin kuten esimerkiksi palvelimeen, verkkolevyyn tai muihin yrityksen laitteisiin. Yhteys onnistuu muodostaa mistä vain, ja liikenne kulkee salattuna asiakaslaitteesta aina VPN-yhteyden päättävään päähän.

VPN-yhteyden muodostamiseen on monia muitakin käyttötapoja. Sen kautta voidaan ajaa muita tietoturvaprotokollia tai salata ohjelmistojen liikenne laitteesta toiseen inter-

netin yli [25, s. 236]. Myös yrityksen intranet- ja extranet voidaan jakaa turvallisesti internetin yli.

VPN-verkkoja on kolmenlaisia: etäyhteysverkot, toimipisteiden väliset ja extranet-verkot. Etäyhteysverkossa asiakaslaitteessa on ohjelma, jolla luodaan yhteys yritysverkossa olevaan laitteeseen. [26, s. 237-238.]

Toimipisteiden välinen verkko tarkoittaa esimerkiksi yrityksen kahden erillään olevan verkon yhdistämistä internetin yli. Toimipisteet voivat sijaita eri maassa ja niiden välinen salattu VPN-tunneli yhdistää verkot keskenään. Käyttäjät pääsevät käyttämään samoja palveluja aivan kuin olisivat fyysisesti samassa verkossa. [27, s. 238.]. Site-to-site VPN on yksi esimerkki tällaisesta verkkojen yhdistämisestä.

The Internet Engineering Task Force (IETF) on määritellyt IPSec:n (IP Security Architecture) dokumenteissaan. Se koostuu useista tietoturvaprotokollista ja salauksista. Tämä teollisuusstandardiksi muodostunut menetelmä toimii OSI-mallin verkkokerroksella. [28, s. 243.] Sen laajojen ominaisuuksien takia sitä hyödynnetään entistä enemmän tiedon salauksessa.

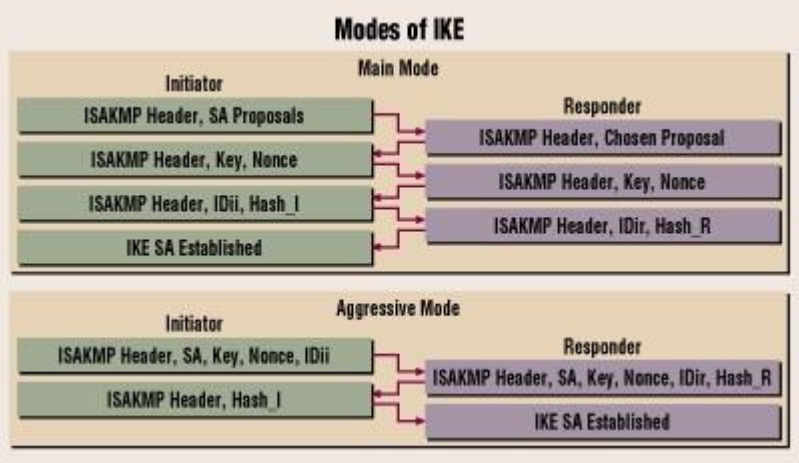
IPSec:ssä salausmuodot ovat tunneli- ja siirtotila. Tunnelitilassa kokonainen IP-paketti kapseloidaan ja suojataan toisen paketin sisään. Kapselointi tehdään yleensä reitittimessä tai palomuurissa ja paketteihin lisätään näiden omat käytettävät IP-otsikot. Tunnelimuodossa voidaan käyttää AH:ta (Authentication Header) ESP:tä (Encapsulating Security Protocol) tai molempia. Siirtomuotoisessa toteutuksessa IP-paketista salataan vain hyötykuorma. Tämän takia se on turvattomampi protokolla tunnelimuotoon verrattuna. [29, s. 248-249.]

ISAKMP eli Internet Security Association Key Management on kehys, jota tarjoaa avaintenvaihtoprotokollan ja tietoturvakäytänteet. Sen avulla pystytään luomaan turva-assosiaatiot (SA) yhteyksille. Yksityisten avaimien luominen ja hallinta sekä niiden turvallinen jakaminen vertaisten välillä onnistuu ISAKMP:n avulla. [30, s. 254.]

IKE (Internet Key Exchange) on protokolla, jolla luodaan luottosuhteet vertaisen välille ja jonka avulla pystytään neuvottelemaan turvakäytänteet. ISAKMP kuuluu osaksi IKE:n käytäntöä. Tämän lisäksi siihen käytetään osittain myös SKEME:n (Secure Key

Exchange Mechanism) ja Oakleyin protokollia yhteyden muodostamisessa. [31, s. 252.]

IKE koostuu kaksivaiheisesta yhteyden luomisesta. Ensimmäinen vaihe on mahdollista toteuttaa joko Main Modessa tai Aggressive Modessa. Kuvan 6 mukaan aggressive modessa jätetään pois IKE-todennuksen vaiheita. Main modessa käydään läpi kaikki todennuksen vaiheet. [32.]



Kuva 6. IKE SA:n muodostamien vaiheessa 1. [33.]

Ensimmäisen vaiheen tarkoitus on muodostaa turvallinen yhteys vertaisten välille ISAKMP-vaihdoilla. Tähän kuuluvat yhteysparametrien neuvottelu, avaintenvaihto Diffie-Hellman protokollalla, todennuspyyntö ja esijaetut avaimet. Ensimmäisestä vaiheesta muodostuu yhteyssopimus nimeltä IKE SA. Tätä kaksisuuntaista sopimusta käytetään hyväksi toisessa vaiheessa IPSec SA:n muodostamista varten. Kaksisuuntaisuus tarkoittaa sitä, että IKE osaa käyttää samoja yhteysparametreja molempiin suuntiin. [34.]

Toisessa vaiheessa käytetään ensimmäisessä vaiheessa luotua tunnelia lisäämällä siihen turvaparametreja. IKE neuvottelee turva-assosiaatiot, ylläpitää niitä sekä toistaa mahdollisesti Diffie-Helman-avainvaihdon riippuen PFS:n (Perfect Forward Secrecy) käytöstä. [35, s. 256-257.] Lopputuloksena muodostetaan IPSec SA -sopimuksia. Näitä sopimuksia neuvotellaan kumpaankin suuntaan vähintään yksi kappale.

Näiden kahden vaiheen jälkeen salattu tunneli on luotu ja sen läpi kulkevaa dataa salataan sopimusten mukaan.

3 Palomuurivaihdon suunnittelu ja asennus

3.1 Suunnittelu

Lähtökohtaisesti kriittisten laitteiden vaihtaminen ja ylläpitäminen, josta voisi olla asiakkaille tai omalle liiketoiminnalle haittaa, pitäisi toteuttaa siten, että siitä syntyy häiriötä mahdollisimman vähän. Tässä tapauksessa palomuurin vaihto toteutetaan ilta-aikaan, jolloin liikennettä ja palveluiden käyttöä on normaalia vähemmän. Asiakkaille, joita tämä laitevaihto koskee, tiedotetaan huoltotöistä. Tarkempaan suunnitelmaan voi tutustua liitteessä 1. Liitteestä selviää myös projektin aikataulu ja muuta taustatietoa.

Palomuuri asennetaan käyttövalmiiksi ennen sen vaihtamista. Tarkoituksena on testata joitakin palveluja etukäteen, jotta vaihto onnistuisi mahdollisimman nopeasti ja ilman häiriötä. Etukäteen testataan asennettujen verkkojen toimivuus, DHCP-protokolla ja virtuaaliset verkot. Fyysiset kytkennät testataan ja verrataan verkkosuunnitelmaan. IPSec-verkkojen asetukset täytyy myös tarkistaa huolellisesti, jotta ne ovat samat etäpisteissä.

Työ toteutetaan Zyxel Zywall 310 -palomuurilla. Kuvassa 7 näkyvät sen ominaisuudet.

Model	ZyWALL 1100	ZyWALL 310	ZyWALL 110
Hardware Specifications			
10/100/1000 Mbps RJ-45 ports	8 (configurable)	8 (configurable)	2 x WAN, 1 x OPT, 4 x LAN/DMZ
USB ports	2	2	2
Console port	Yes (DB9)	Yes (DB9)	Yes (DB9)
Rack-mountable	Yes	Yes	Yes
System Capacity & Performance*1			
SPI firewall throughput (Mbps)*2	6,000	5,000	1,600
AES VPN throughput (Mbps)*3	800	650	400
Unlimited user licenses	Yes	Yes	Yes
Max. concurrent sessions*4	500,000	100,000	60,000
New session rate	12,000	12,000	3,500
Max. concurrent IPsec VPN tunnels	1,000	300	100
Max. concurrent SSL VPN users	250	50	25
Included SSL VPN user no.	250	50	25
Customizable zones	Yes	Yes	Yes
IPv6 support	Yes	Yes	Yes

Kuva 7. Zywall 310 -ominaisuudet. [36.]

Palomuurin etuja ovat nopeat gigabitin liitännät, VPN-yhteyksien läpäisykyky, SSL-VPN-yhteyksien määrä sekä rajoittamattomat käyttäjälisenssit. Vanhaan Zyxel Zywall 300:een verrattuna teholisäystä on huomattavasti.

3.2 Perusasetukset

Palomuurin asennus lähtee käyntiin firmwaren päivittämisestä. Firmwaresta laitetaan viimeisin versio (4.10 AAAB.0; C0), joka on sillä hetkellä saatavilla. Sen jälkeen lähdetään laittamaan perusasetuksia mm. laitteen nimi, aika-asetukset, hallintakäyttäjän salasanan vaihto ja nimipalvelinosoitteet. Nimipalvelinosoitteeksi (DNS) laitetaan operaattorin ja Googlen nimipalveluosoitteet.

Seuraavaksi luodaan käyttäjätilejä palomuurin hallintaan ja VPN-yhteyksien käyttöön. VPN-yhteydet laitetaan yrityksen henkilöstölle ja niiden tunnuksille määritellään käyttäjätason oikeudet eli ns. user-oikeudet. User-oikeuksilla pystytään tunnistautumaan ja käyttämään verkkopalveluja selaimella, Telnetillä tai SSH:lla. Tämä on käyttäjille riittävä taso eikä heillä ole pääsyä palomuurin hallintaan.

Limited-admin-tunnus luodaan tilanteita varten, jossa palomuuriasetuksia pitäisi päästä katsomaan, mutta käyttäjällä ei ole oikeuksia tehdä muutoksia. Yrityksessä palomuurien ylläpito ovat tiettyjen henkilöiden vastuulla, jotta pystytään estämään muiden käyttäjien tahalliset tai tahattomat muutokset. Käyttäjätunnuksien ominaisuuksista voi lukea liitteen 1 taulukosta 5.

Palomuurin hallintaan tehdään muutos, jonka mukaan ainoastaan suojattu HTTPS-yhteys sallitaan porttiin 47680. Portti on mielivaltaisesti valittu, ja se estää enimmät kirjautumisyritykset laitteeseen. Web-hallintaan kirjautuminen tulee sallia myös palomuuriasetuksista. Kuvassa 8. näkyy web-pohjaisen kirjautumisen portti. HTTP-yhteyksiä ei sallita vaan ne ohjataan käyttämään salattua HTTPS-yhteyttä.

Kuva 8. HTTPS-yhteyden hallintaportin asettaminen.

3.3 Lähiverkot

Alkuasetuksien jälkeen luodaan palomuuriin tarvittavat lähiverkot. Yrityksen käyttöön ja eri palveluille määritellään omat verkkonsa. Asiakasverkot toteutetaan virtuaalilähiverkon ja eri vyöhykkeiden avulla, jotta niiden hallinta on helpompaa jatkossa. Lisäksi ne täytyy eristää toisista verkoista tietoturvasyistä.

Palveluverkon IP-osoitealuetta ei ole muutettu yrityksessä, sillä silloin olisi pitänyt muuttaa kaikkien sisäverkon laitteiden IP-asetukset. Palveluverkossa sijaitsee yrityksen keskeisimpiä palveluita kuten posti- DNS- ja tiedostopalvelut, joiden toiminta halutaan taata myös palomuurivaihdoksen jälkeen.

Palveluverkon asetukset laitetaan kuvan 9 mukaisesti. Liitännän 1 IP-osoite määritellään 192.168.10.1 aliverkon maskilla 255.255.255.0. Sisäiseksi DNS-palvelimeksi määritellään 192.168.10.15 ja julkiset DNS:t ovat 193.210.19.19 ja 193.210.18.18. Ulospäin menevää kaistaa ei tarvitse rajoittaa, vaan se jätetään oletukseksi.

Kuva 9. Palveluverkon IP- ja DHCP-asetukset.

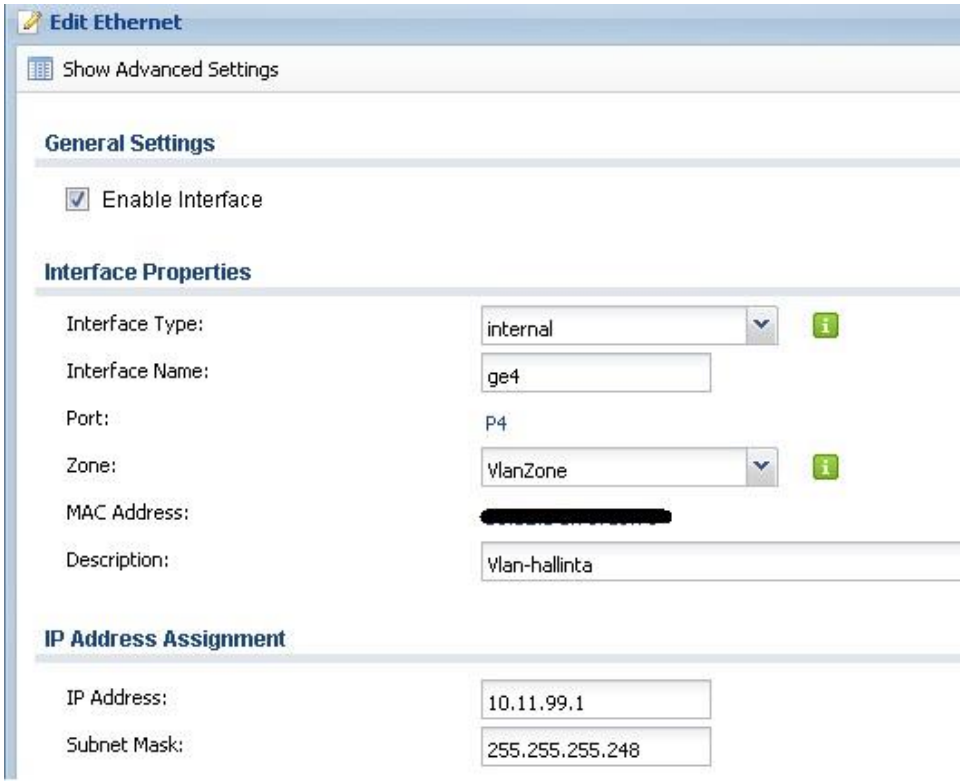
Palomuurin viimeiseen porttiin määritellään julkisen verkon osoitteet. Käytössä on osoiteavaruus maskilla 255.255.255.240. Tähän mahtuu 14 osoitetta. Verkko-osoite on 193.87.45.64, josta viimeinen osoite 193.87.45.78 tulee palomuurin käyttöön.

Etähallittavalle palvelimelle luodaan verkko 10.10.150.0 /24. Se määritellään liitäntään 7. ja IP-osoitteeksi määritellään 10.10.150.254. Tälle verkolle jaetaan DHCP:llä viisi IP-osoitetta osoitteesta 10.10.150.10 lähtien.

3.4 Virtuaalilähiverkot

Virtuaalilähiverkot otetaan käyttöön, koska ne eivät vaadi fyysisiä lisäkytkentöjä, ne lisäävät tietoturvaa ja verkon törmäysalueita saadaan rajattua. Toimisto- ja asiakasverkot tehdään virtuaalisten verkkojen avulla.

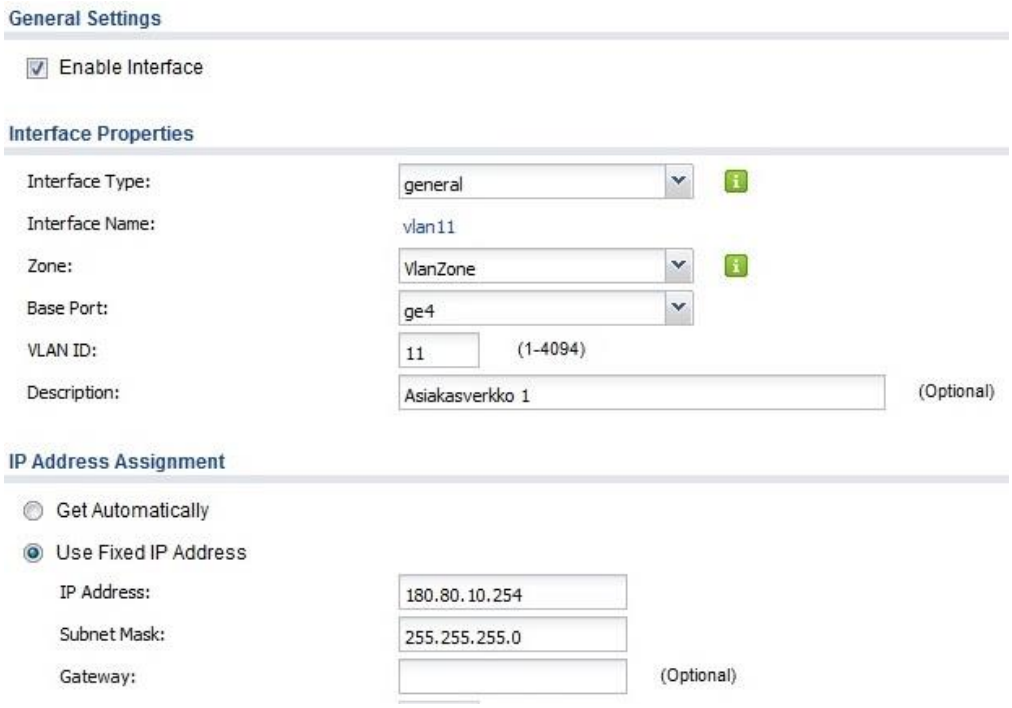
Palomuurissa kaikkien virtuaaliverkkojen välitysportiksi määritellään liitäntä 4. Sen kautta välitetään kaikki VLAN-informaatiot kerroskytkimille. Zyxelin palomuurissa liitäntä saadaan käyttöön luomalla sille joku erillinen hallintaverkko. Ilman IP-osoitteita ei liitäntää pysty muuten ottamaan käyttöön. Kuvassa 10 näkyvät hallinta-VLAN:n asetukset. Tässä verkossa ei jaeta IP-osoitteita.



Kuva 10. VLAN-hallintaverkon IP-osoitetiedot

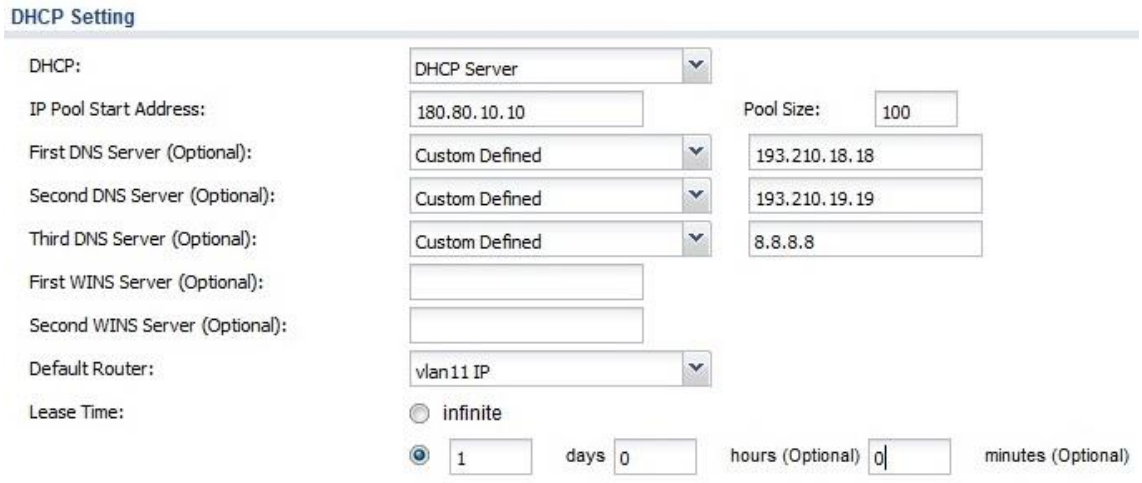
Tässä näytetään vain kahden virtuaaliverkon luominen, koska muut verkot asennetaan samalla tavalla. VlanZone-vyöhyke valitaan jokaiseen VLAN:iin samaksi.

Asiakasverkko 1 luodaan Vlan:iin 11 (kuva 11). Verkon IP-osoite on 180.80.10.254 ja maski 255.255.255.0.



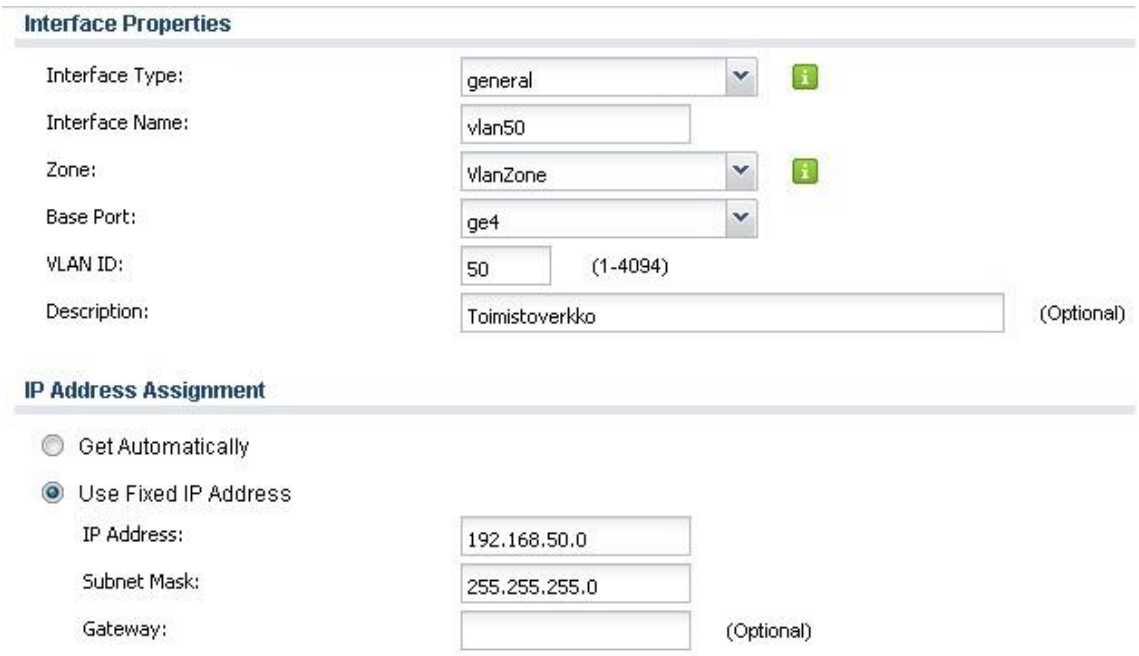
Kuva 11. Asiakasverkko 1 -asetukset.

Verkolle asetetaan DHCP (kuva 11), ja se jakaa 100 osoitteita alkaen osoitteesta 180.80.10.10. IP-osoitteiden vuokra-aika säädetään yhden päivän mittaiseksi, jotta osoitteet eivät lopu. Jos tätä aikaa ei määritetä, vuokrausmäärät voisivat tulla täyteen, jolloin uudet laitteet eivät saisi enää IP-osoitteita. Voidaan myös olettaa, että verkossa ei ole 100 laitetta yhtä aikaa aktiivisena.



Kuva 12. Asiakasverkko 1. DHCP-asetukset.

Toinen VLAN-verkko on toimistoverkko, joka asennetaan virtuaalilähiverkkoon 50 kuvan 13. mukaisesti. VLAN-liitännän IP-osoitteeksi valitaan 192.168.50.254 maskilla 255.255.255.0. DHCP määritellään jakamaan 30 osoitetta osoitteesta 192.168.50.20 alkaen. Oletusyhdyskäytävää ei näissä tapauksissa tarvitse määrittää, koska IP-verkot reititetään internetiin päin.



Kuva 13. Toimistoverkon asetukset palomuurissa.

VLAN:en toimivuus pystytään testaamaan Ping-testillä, jossa kaksi tietokonetta kytketään samaan tai eri VLAN:iin ja tarkkaillaan Ping-vastauksien saamista. Tarkoituksena on tarkistaa, että palomuuri jakaa oikeat VLAN-verkot ja ne toimivat halutulla tavalla. Liikenne eri VLAN:en välillä estetään. Liitteessä 2. on esitelty tarkemmin testikoneiden verkkoasetukset ja niiden välinen toimivuus eri testikokoonpanoilla.

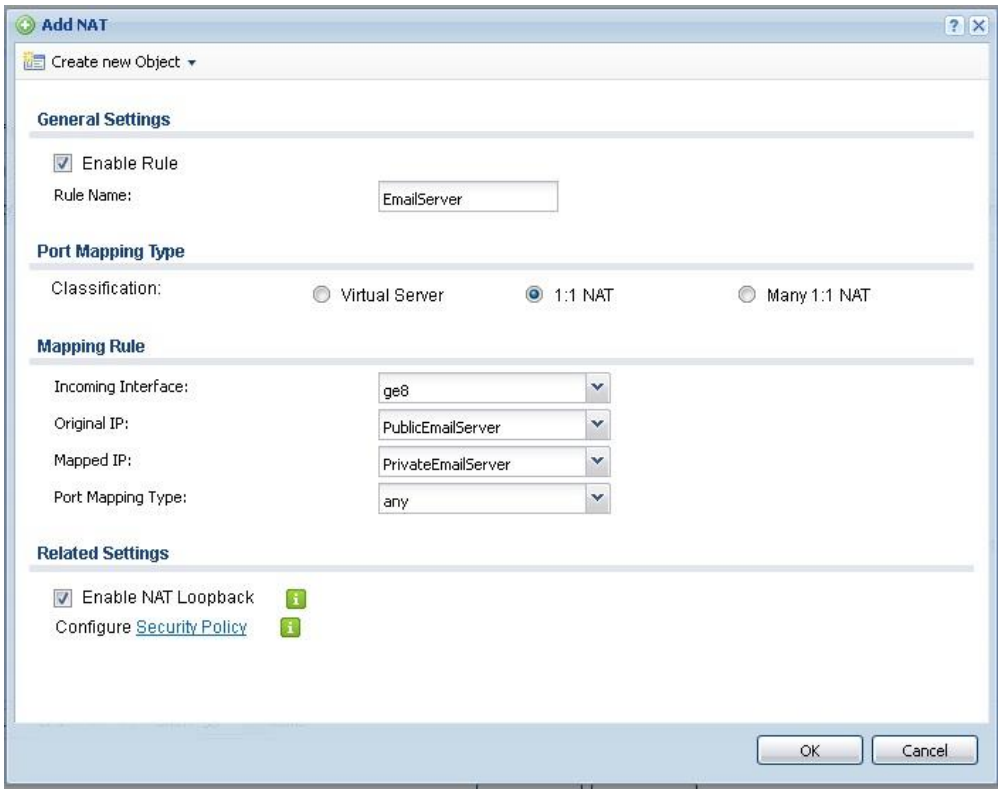
Testausta varten asennettaan HP Procurve 2512 -kytkin, jonka asetukset löytyvät liitteestä 2. Kytkin liitetään palomuurin porttiin 4. Kytkimen portit 1. ja 2. asetetaan VLAN-alueeseen 11. ja portit 3. ja 4. alueeseen 50. Kaikki VLAN-verkot välitetään portin 12. kautta.

Ensimmäisessä testissä tietokoneet kytketään samaan VLAN-alueeseen liitteen 2 mukaan, jolloin ne pystyvät kommunikoimaan keskenään. Toisessa testissä koneet liitetään eri VLAN-alueisiin, jolloin liikennettä ei näiden laitteiden välillä kulje.

3.5 Osoitemuunnos ja porttiohjaukset

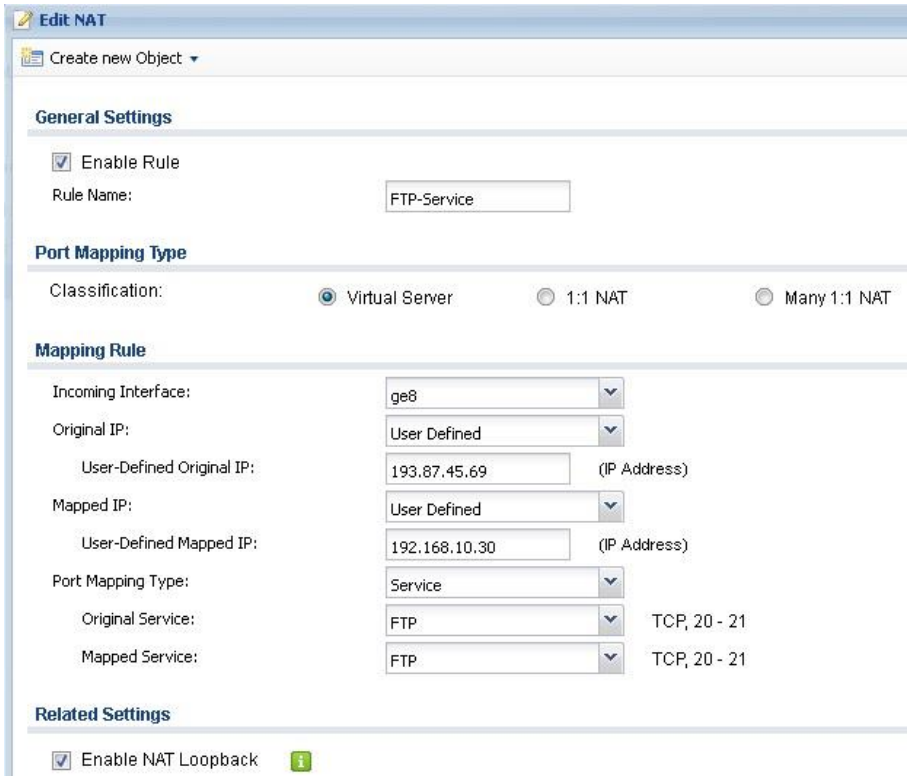
Osoitemuunnoksella pystytään muuttamaan yrityksen ulkoverkon IP-osoite sisäverkon osoitteeksi. Nämä muutokset tehdään 1:1 NAT -tekniikalla. Esimerkiksi postipalvelimen julkinen IP-osoite 193.87.45.65 muutetaan osoitteeksi 192.168.10.10. Porttiohjauksia ei tehdä. Koska postipalvelimen osoite ei näy ulospäin eivätkä käyttäjät sitä voi tietää, luo se paremman turvallisuuden ja estää monenlaisia hyökkäystapoja. NAT Loopback -ominaisuus pidetään päällä, jotta palomuurin sisäverkosta tulevat yhteydet pystytään avaamaan postipalvelimeen.

Kuten kuvasta 14. nähdään, NAT 1:1 -asetus laitetaan päälle. Liikenne tulee liitännän 8. kautta. PublicEmailServer-nimi viittaa postipalvelimen julkiseen ja PrivateEmailServer sisäiseen IP-osoitteeseen.



Kuva 14. 1:1-osoitemuunnos postipalvelimelle.

Virtual Server tarkoittaa samaa kuin porttiohjaus, ja se otetaan käyttöön NAT-asetuksista. Sillä ohjataan web-palvelimeen tulevat yhteydet oikeisiin portteihin. Esimerkiksi FTP-palvelua käytetään internetistä sisäverkkoon porttien 20 ja 21 kautta. Nämä portit ohjataan samoihin portteihin eteenpäin. Kuvassa 15 näkyvät porttiohjauksen asetukset.



Kuva 15. Porttiohjauksen tekeminen.

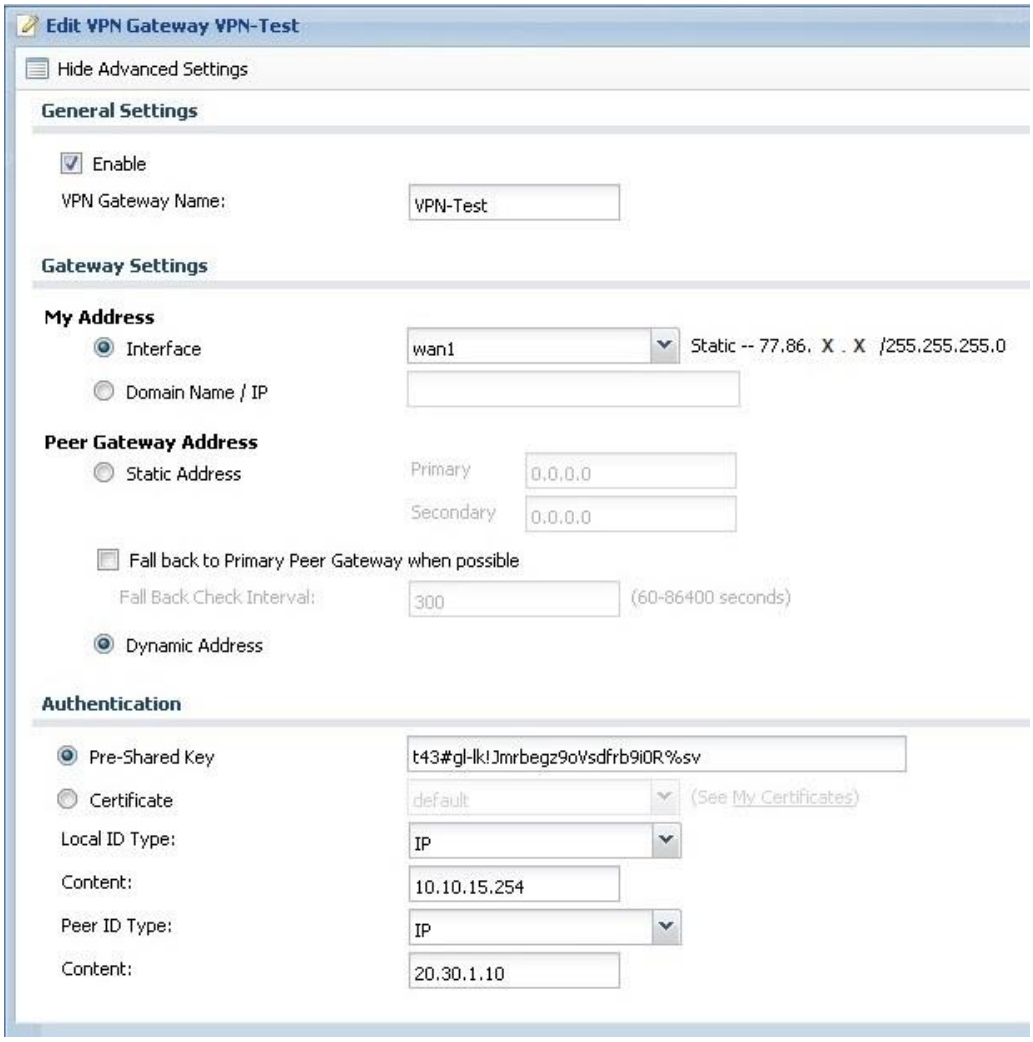
On olettavaa, että julkiset IP-osoitteet loppuvat yrityksen osoiteavaruudesta ennemmin tai myöhemmin. Tällöin käytetään porttiohjausta tehokkaammin hyväksi, jolloin samaa julkista osoitetta voidaan käyttää monen laitteen ja palvelun kanssa.

3.6 IPSec VPN-yhteydet

Palveluverkon käyttäminen ja ylläpitäminen etäyhteydellä tehdään IPSec-pohjaisella VPN:llä. Yhteys muodostetaan asiakaslaitteesta palomuuriin erillisen ohjelmiston avulla. Ohjelmistona käytetään Shrew Softin Access Manager -ohjelmaa. Yhteydet luodaan ja testataan tällä ohjelmalla. Koska ohjelmaan tulee samat asetukset kuin palomuuriin, niitä ei käsitellä tässä erikseen. Tarkat asiakaslaitteen asetukset löytyvät liitteestä 3.

Palomuuriin luodaan 10.10.15.0 /24 -verkko etäyhteyttä varten, ja paikallinen verkko on 192.168.50.0 /24. Sen jälkeen määritellään palomuuriin kuvassa 16. näkyvät asetukset. Oletusreitiksi valitaan WAN (Wide Area Network) -liitäntä, laitetaan jaettu salainen

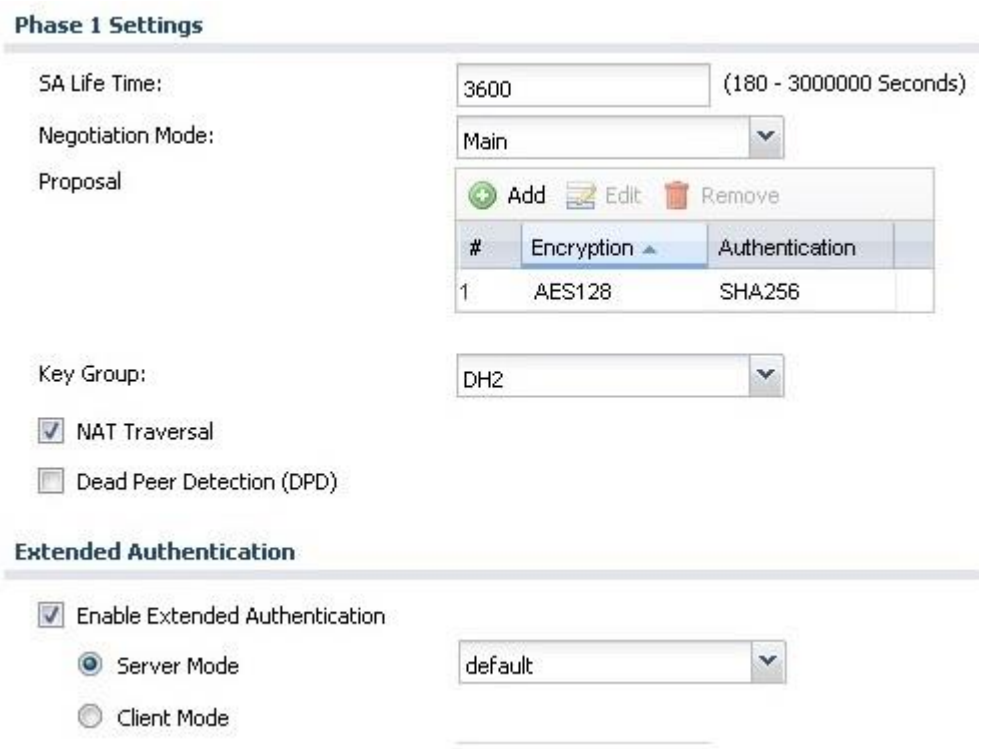
avain ja identiteettiosoitteet. Identiteettiosoitteilla saadaan lisättyä verkon turvallisuutta ja niiden täytyy vastata niin asiakaspäässä kuin palomuurissakin.



Kuva 16. IPSec VPN-yhteyden salattu avain ja ID-tunnisteet.

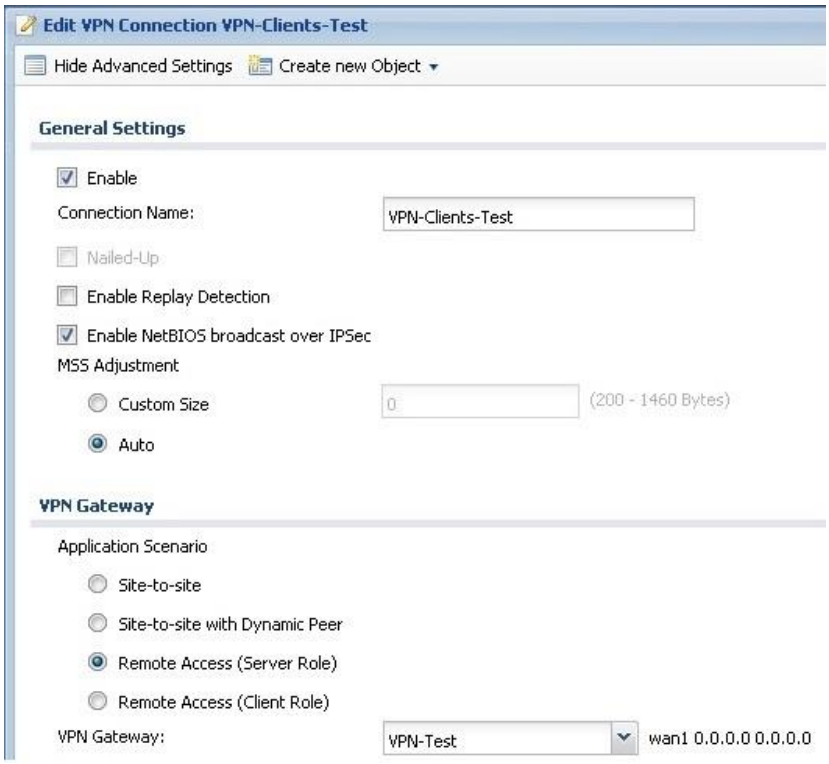
Vaiheessa 1 määritellään turva-assosiaatio ja sen elinikä. Elinikä laitetaan 3600 sekuntiin eli yhteen tuntiin. Tämän jälkeen yhteys luodaan uudelleen, jos se on vielä avoin.

Testi-VPN-yhteyden kanssa 192-bittistä AES-salausta ei saatu toimimaan. Tämän vuoksi valitaan 128-bittiinen salaus, joka on riittävän hyvä ja turvallinen nykyajan tarpeisiin. Tiivisteeksi valitaan turvallinen SHA256. Avaintenvaihtomenetelmänä pidetään 1024-bittistä DH2:sta.



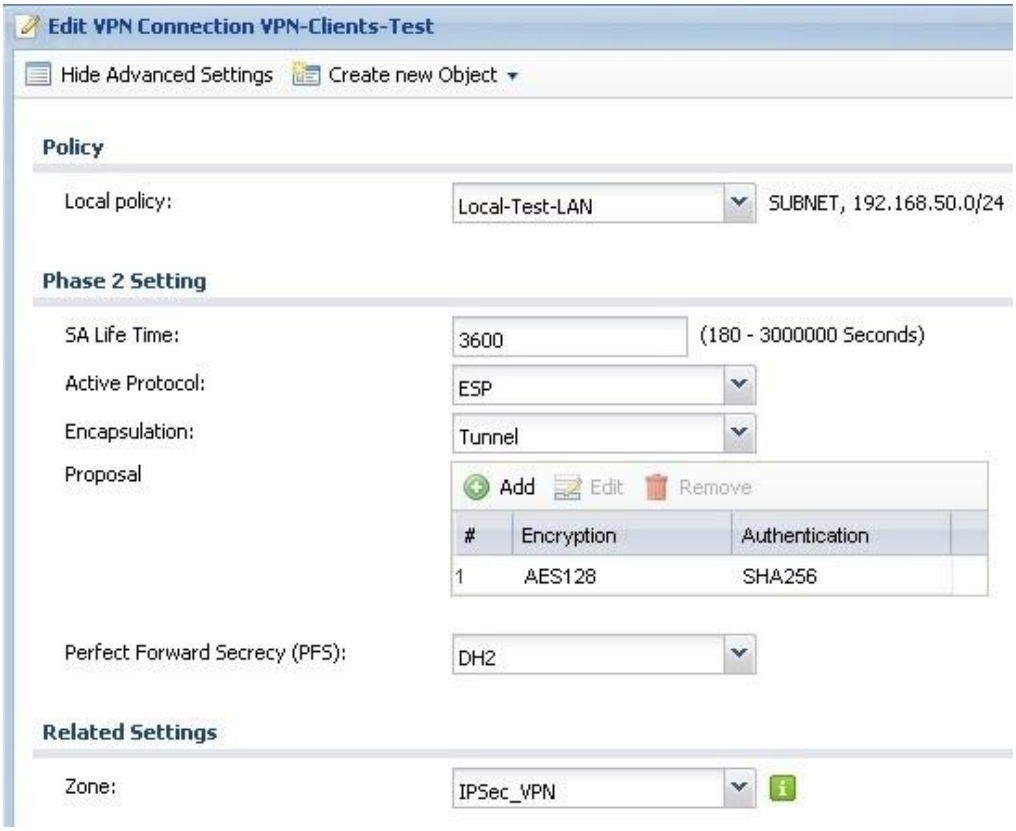
Kuva 17. IKE:n ensimmäisen vaiheen asetukset.

Seuraavaksi määritellään IKE:n vaiheen 2. asetukset sekä määritellään VPN-yhteyden rooli. Palomuuri laitetaan kuvan 18. mukaan Remote Access (Server Role) -tilaan, jotta siihen tulevat yhteydet voidaan päättää. Yhdyskäytävänä käytetään aiemmin luotua WAN-liitäntää.



Kuva 18. VPN-yhteyden oletusyhdyskäytävä ja palvelinrooli.

Kuvassa 19. yhteyden turvallisuutta lisätään IKE-vaiheessa 2. Data kapseloidaan tunnelimuodossa ESP-protokollaa käyttäen. Lisäksi käytetään samoja salaus- ja tiivistysalgoritmeja kuin vaiheessa 1.

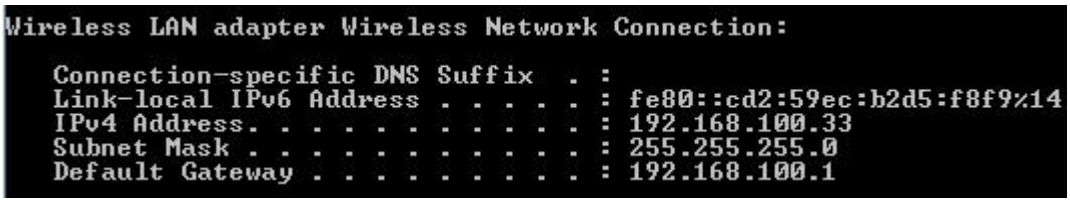


Kuva 19. IKE vaihe 2. -asetukset.

Testiyhteyttä varten tehdään tarvittavat muutokset palomuurisääntöihin, jotta yhteys toimisi oikein. Näiden asetuksien jälkeen voidaan testata yhteyttä Ping-komennon avulla. Ping-komento lähettää ICMP echo request -paketin. Jos vastaanottava laite saa paketin, se vastaa siihen echo reply -paketilla.

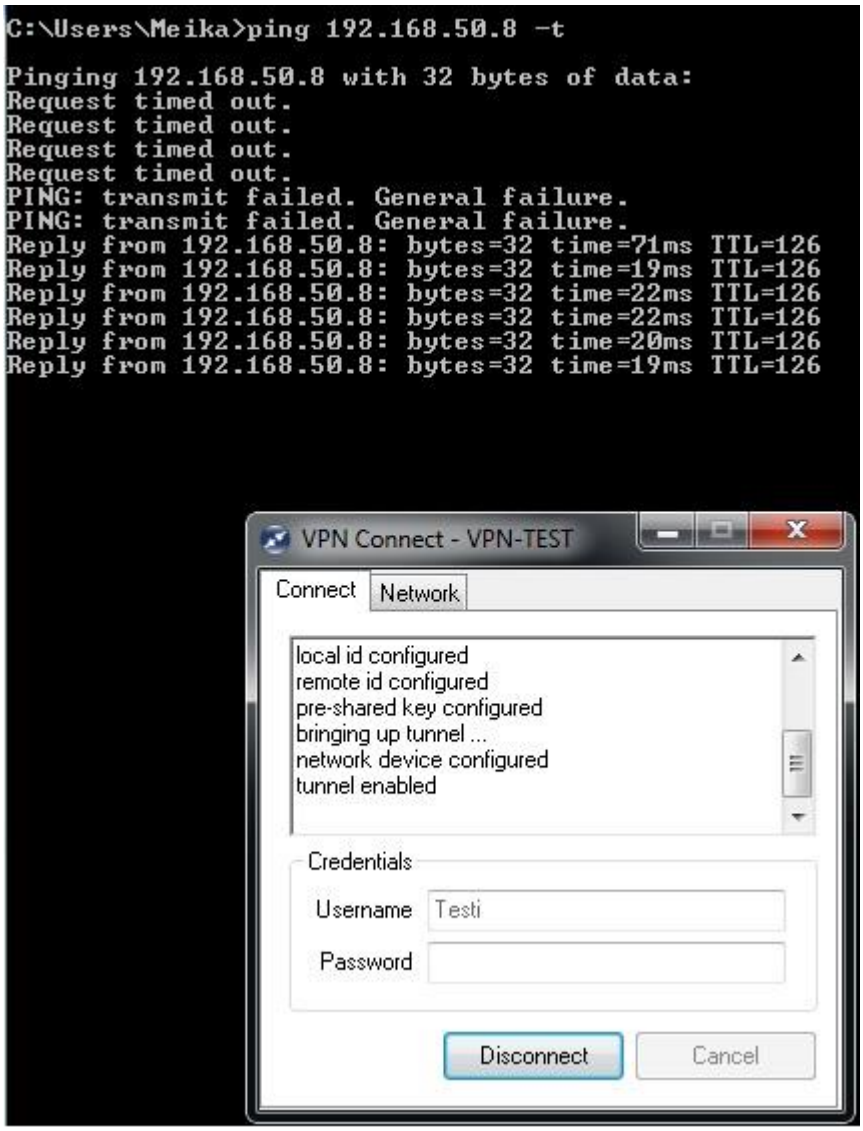
Kuvassa 21 näkyy Access Manager -ohjelman ikkuna. Palomuuri asetetaan testausta varten julkisen verkon rajapintaan ja siihen otetaan yhteys internetistä päin.

Ping-komennolla lähetetään paketteja ennen VPN-yhteyden luomista (kuva 20). Vastausta haetaan etäverkossa olevalta laitteelta, jonka IP-osoite on 192.168.50.8. Oman testiverkon tiedot näkyvät myös kuvassa 20. IP-osoite on 192.168.100.33 ja aliverkon maski 255.255.255.0.



Kuva 20. Testikoneen verkon asetukset.

Kuten kuvasta 21 voidaan huomata, että aluksi etälaite ei vastaan Ping-komentoon ollenkaan, koska yhteyttä etäverkkoon ei ole luotu. Kun VPN-tunneli saadaan avattua (Tunnel enabled), saa testikone vastauksen etälaitteelta. Kuvassa 21 näkyy myös osittain tunnelin luomisessa käytävä proseduuri, jossa yhteys neuvotellaan palomuurin kanssa.



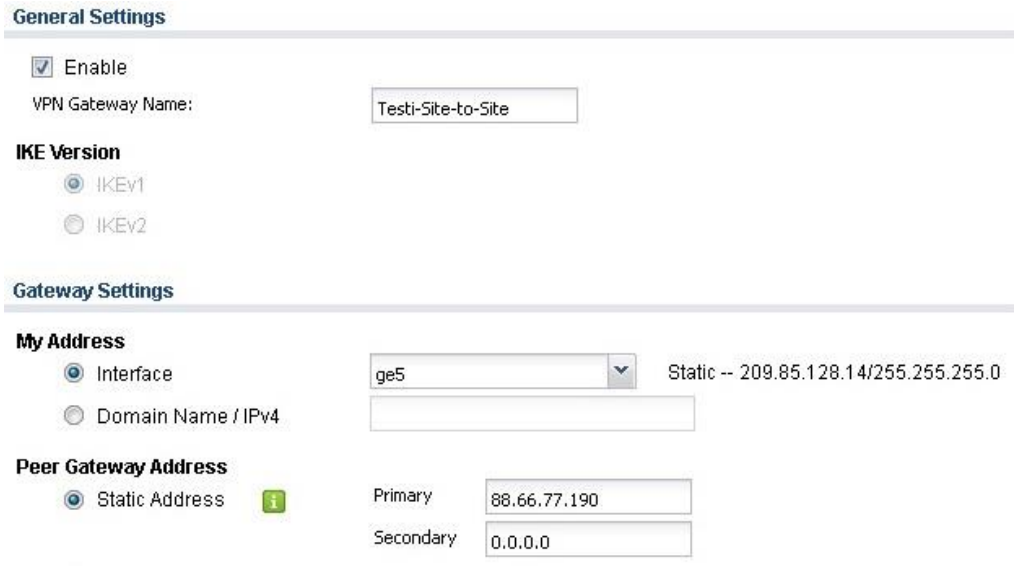
Kuva 21. Laitteen vastaaminen Ping-komentoon VPN-yhteyden ollessa päällä.

VPN-yhteydellä yhdistetään myös eri verkot internetin yli. Tarkoituksena on tehdä turvallinen ja salattu tunneli palomuurien välille Site-to-site-menetelmällä. Liikenteeseen on vaikea päästä väliin eikä sitä pysty tarkkailemaan. Tunnelissa voidaan kuljettaa asiakkaan varmuuskopiot sekä hallita ja valvoa etäältä laitteiden ja palveluiden toimintaa.

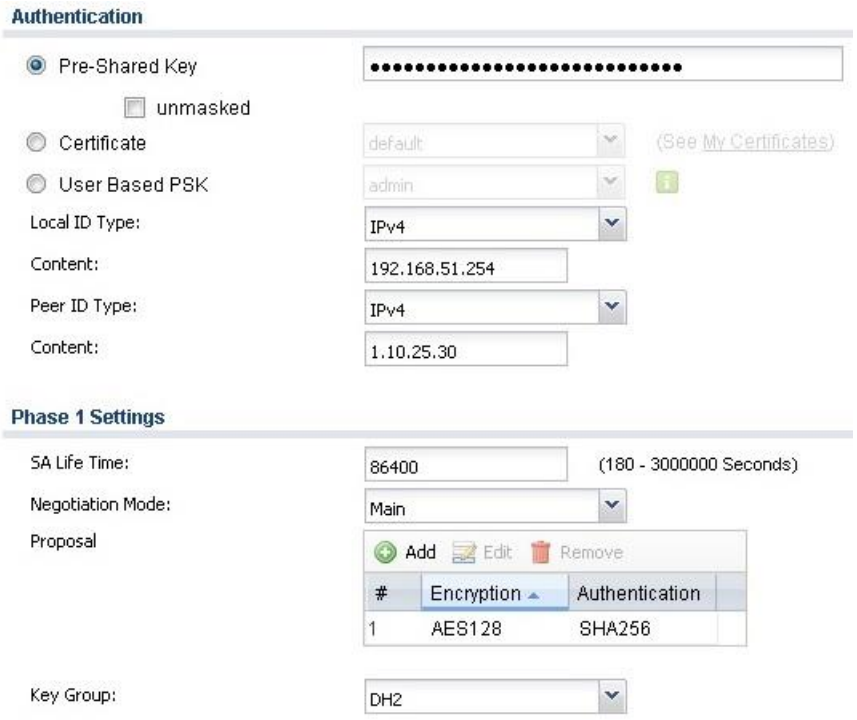
VPN-yhteys toteutetaan kahden palomuurin välille siten, että asiakkaan etätoimipisteestä luodaan yhteys yrityksen sisäverkkoon. Asiakkaan sisäverkko ja yrityksen palomuurin taakse asennettava oma verkko yhdistetään tunnelilla. Näin asiakas pystyy käyttämään yrityksen sisäverkossa olevaa laitetta.

Kuvissa 22 ja 23 näkyvät yhdyskäytäväpään asetukset. Yhteyden vastapään osoite on 88.66.77.190. Yhteys neuvotellaan Main-tilassa 24 tunnin välein käyttäen AES-salausta ja SHA256-tiivistefunktiota. Neuvottelussa käytetään IKE:n versiota 1, koska vastapään laite ei osaa käsitellä versiota 2.

IKE:n versioissa 1 ja 2 on joitakin eroavaisuuksia. IKE versio 2 ei vie kaistaa niin paljon, ja se tukee EAP-tunnistusprotokollaa jaetun salausavaimen ja sertifikaatin lisäksi. On myös edistyksellistä, että versio 2 osaa tunnistaa, onko tunneli edelleen pystyssä, ja se tukee NAT Traversal (NATT tai NAT-T) -ominaisuutta. [37.] NAT Traversalin avulla pystytään IPSec-pohjaisia paketteja välittämään eteenpäin NAT:n läpi. Ominaisuus lisää uudet lähde- ja kohdeporttikentät, joita se käyttää paketin välittämiseen. NATT käyttää UDP:tä porttiin 4500. [38.]

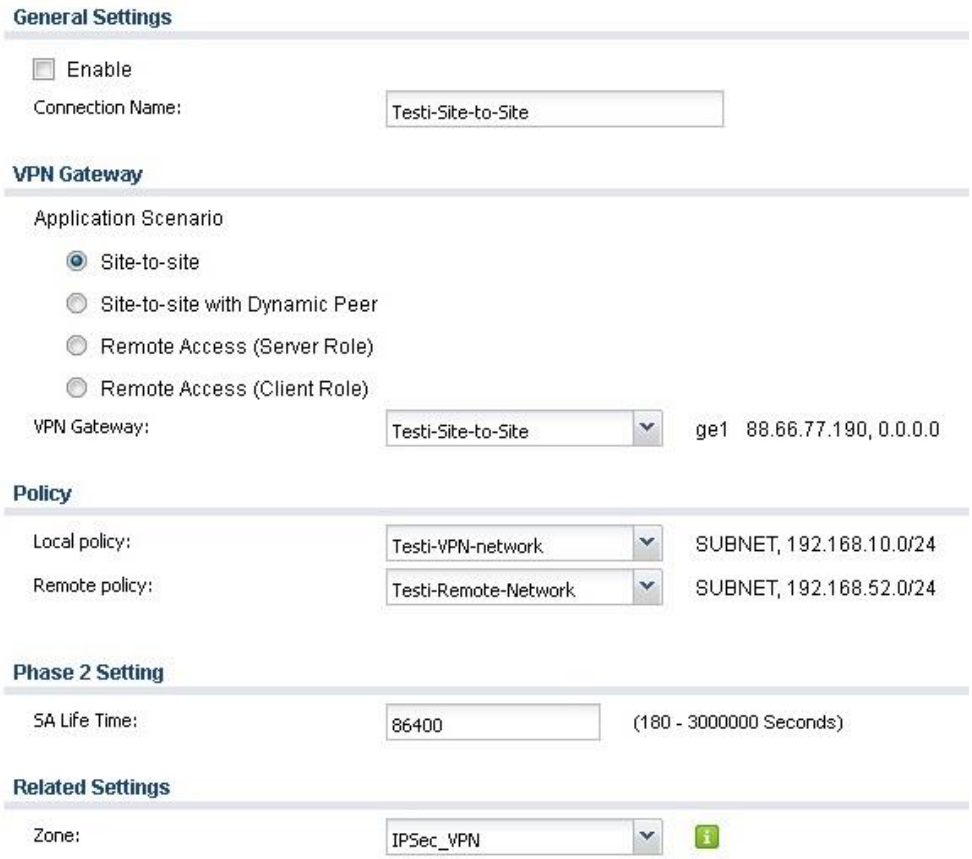


Kuva 22. Oletuskäytävän asetukset Site-to-site-VPN:ssä.



Kuva 23. ID-tyypit ja vaihe 1 -asetukset site-to-site VPN:ssä.

Vaiheessa 2. valitaan rooliksi Site-to-site (kuva 24). Paikalliseksi verkoksi asetetaan 192.168.10.0/24 ja etäverkoksi vastapään lähiverkko 192.168.52.0/24. Vaiheessa 2 käytetään samoja salaus- ja tiivistysalgoritmeja: AES128:sta ja SHA256:sta. Nämäkin asetukset neuvotellaan 24 tunnin välein.

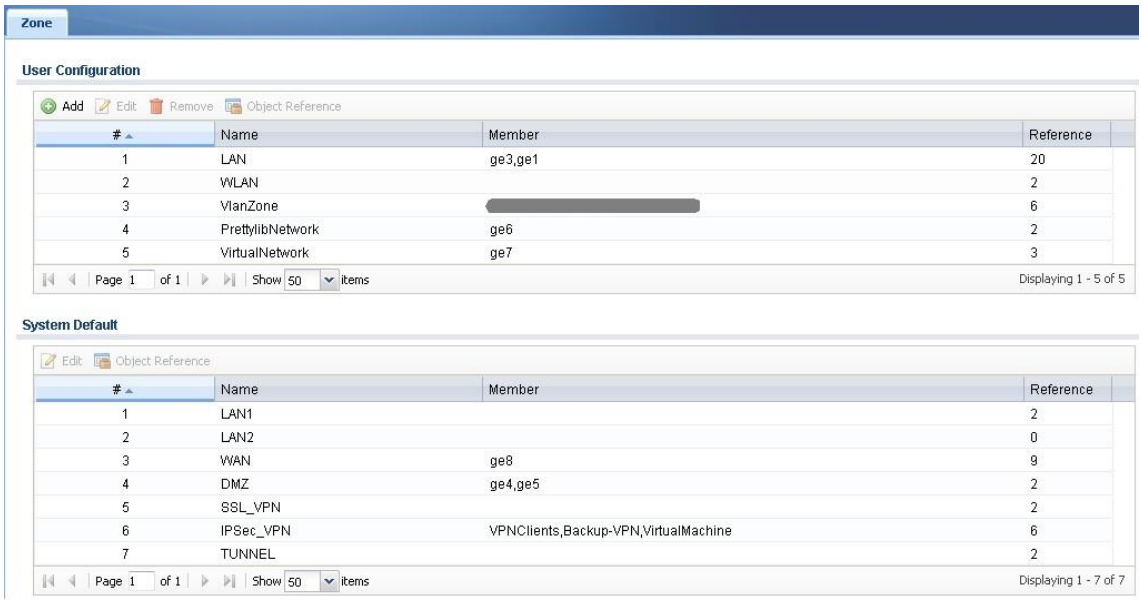


Kuva 24. Asiakas-site-to-site-yhteyden asetuksia.

3.7 Vyöhykkeet

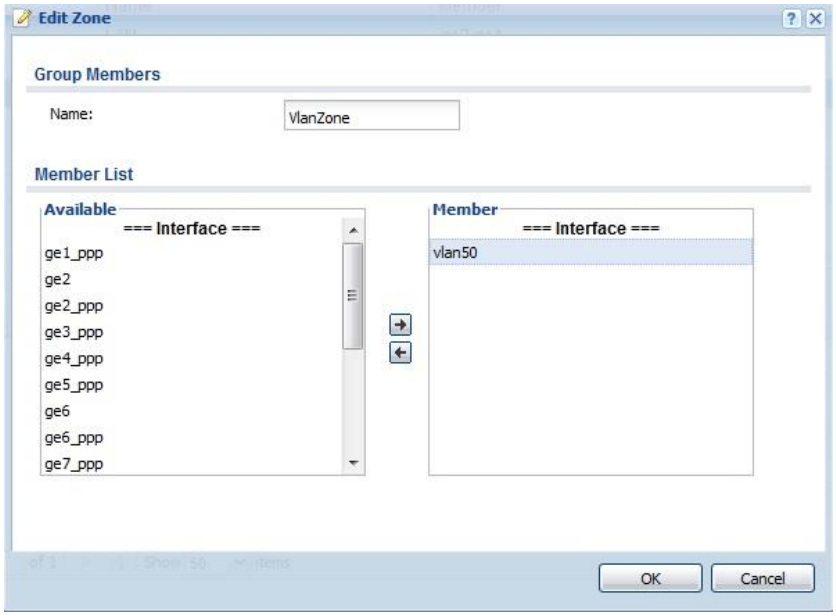
Vyöhykkeitä hallinnoidaan Zone-välilehdellä (kuva 25), jolla pystytään määrittämään, mihin ryhmiin eri liitännät kuuluvat. Näitä asetuksia muokataan työn edetessä, mikäli on tarpeen. Vyöhykkeillä pystytään hallitsemaan suurempia kokonaisuuksia, mitä liikennettä päästetään ja mihin suuntaan.

Vyöhyke LAN:iin kuuluu palveluverkko, ja sen liitännän porttinumero on yksi. Kuvassa 25 näkyvä liitäntä kolme (ge3) on asennusta varten, ja se on tarkoitus poistaa palomuurin käyttöönotossa. VLAN- ja Kirjastoverkot sekä VPN- ja virtuaaliverkot eriytetään omiin vyöhykkeisiinsä. VlanZone sisältää Asiakasverkko1:n ja Toimistoverkon.



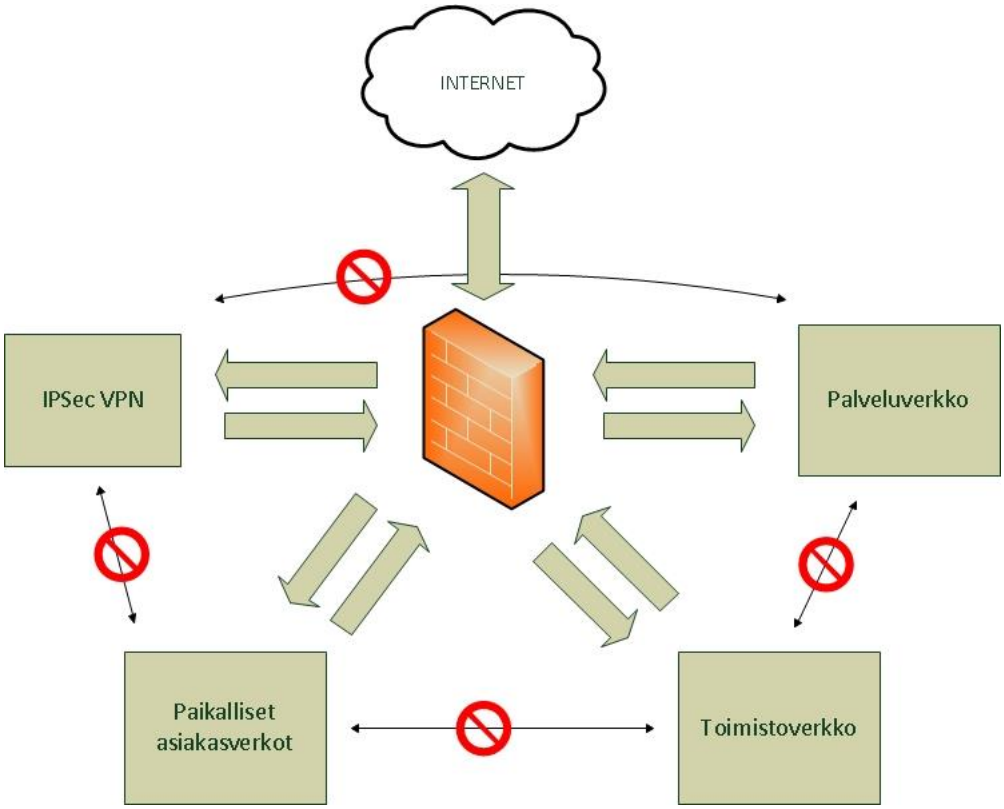
Kuva 25. Palomuurin vyöhykkeet.

Vyöhykkeisiin pystytään lisäämään jäseniä kohdasta Add. Kuvassa 26 on esimerkki toimistoverkon liittämisestä VlanZone-vyöhykkeeseen. Liitännät määritellään yleensä suoraan jo verkkojen luontivaiheessa tiettyyn alueeseen, joten näiden säätäminen on hyvin vähäistä.



Kuva 26. Toimistoverkon lisäys VlanZone-alueeseen.

Yleisesti vyöhykkeistä sallitaan poispäin kaikki liikenne, mutta sisäänpäin liikennettä rajoitetaan. Vyöhykkeiden välinen liikenne estetään kokonaan (kuva 27). Nuolet kuvaavat liikenteen kulkemista sisään ja ulos.



Kuva 27. Vyöhykkeiden välinen liikenne.

3.8 Palomuurisäännöt

Palomuurisääntöjä ohjataan Policy Control -säännöstöllä. Sillä pystytään rajoittamaan ja hyväksymään verkot ja protokollat, joita yhteydet voivat käyttää liikennöidessään palomuurin läpi. Seuraavassa on koottu keskeisimpiä sääntöjä, jotka koskevat aiemmin luotuja verkkoja ja palveluita.

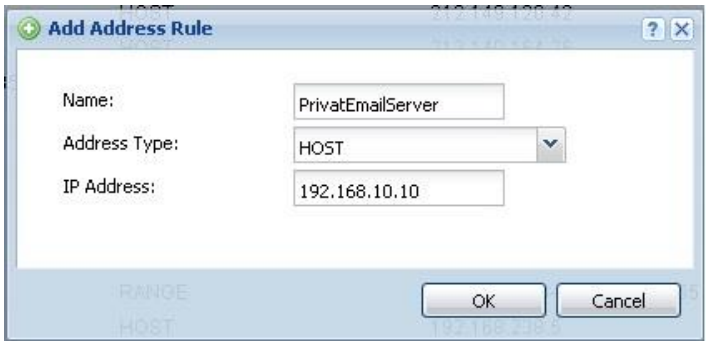
Palomuurisääntöjen tekemisessä ajatuksena on: mikä ei ole sallittua, on kiellettyä. Tämä toteutetaan siten, että palomuurin viimeinen sääntö kieltää kaiken.

From	To	IPv4 Source	IPv4 Destinati...	Service	User	Schedule	Action	Log
any	any	any	any	any	any	none	deny	log

Kuva 28. Viimeinen palomuurisääntö kieltää kaiken.

Kuten kuvasta 28. näkyy, kaikki lähde- ja kohdeosoitteet sekä protokollat otetaan säännössä huomioon ja kielletään deny-komennolla. Palomuurisäännöt suoritetaan järjestyksessä ylhäältä alas, jolloin sääntöjen järjestyksellä on väliä.

Ennen uuden säännön tekemistä luodaan uudet verkko- ja laiteobjektit. Objektilla voidaan hallita esimerkiksi yksittäistä laitetta, jolla on IP-osoite. Sille annetaan myös nimi, joka helpottaa niiden käsittelemistä. Objektit löytyvät Address-kohdasta Object-valikosta.



Kuva 29. Osoiteobjektin lisääminen.

Kuvassa 29 on esimerkki sisäverkon postipalvelimen objektin lisäämisestä. Address Type -kohdasta pystytään valitsemaan yhden isäntäosoitteen lisäksi aliverkko, tarkka IP-alue sekä erikseen liitännän IP-osoite ja tämän aliverkko sekä oletusyhdyskäytävä.

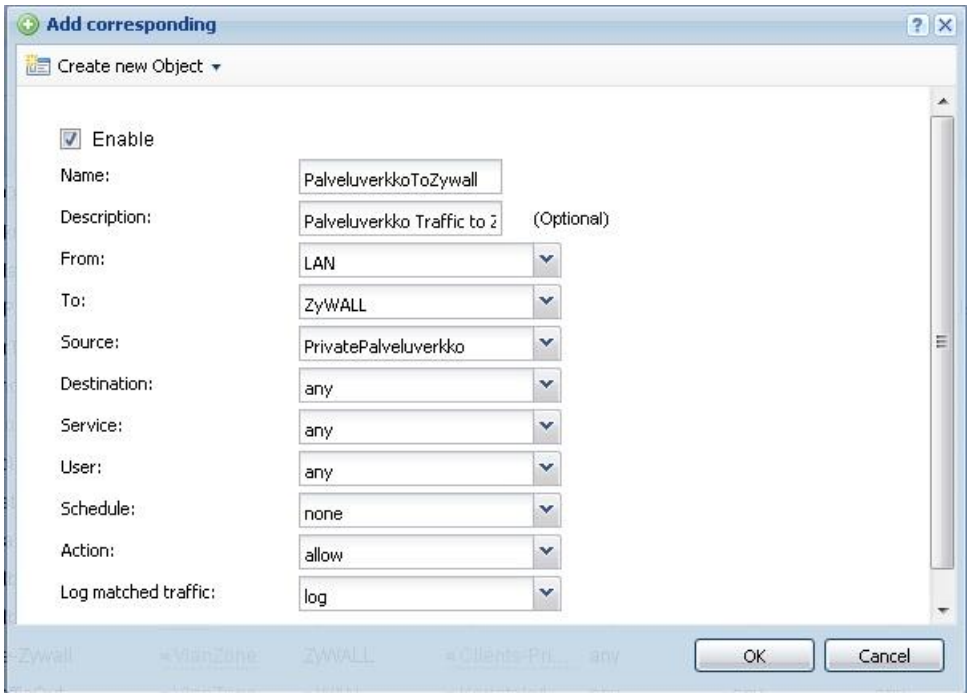
Uusi verkko-objekti luodaan valitsemalla Address Type -kohtaan Subnet (kuva 30).

Kuva 30. Asiakasverkko1-objektin lisääminen.

Palomuurisääntöjä hallinnoidaan välilehdestä Policy Control (kuva 31). Ensimmäiseksi tehdään palomuurin hallintasäännöt, jotta siihen päästään kirjautumaan halutuista verkoista ja vyöhykkeistä. Add-painikkeella lisätään uusi sääntö.

Kuva 31. Policy Control -näkymä ja säännön lisääminen.

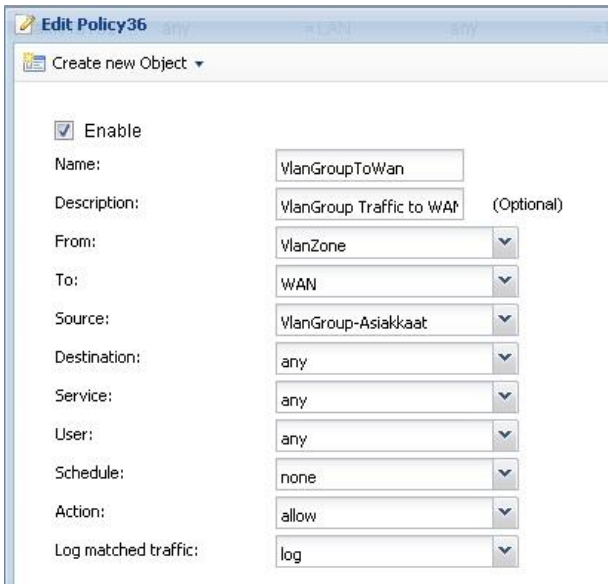
Palveluverkosta (kuvassa nimi PrivatePalveluverkko) 192.168.10.0 /24 sallitaan pääsy kaikilla protokollilla palomuuriin päin kuvan 32 mukaan. Yhteysyrityksistä pidetään lokia, ja tämä valitaan kohdasta Log matched traffic. Sääntö varmistaa sen, että palomuuriin pääsee kirjautumaan https-osoitteella porttiin 47680.



Kuva 32. Sääntö, jonka avulla pääsee palveluverkosta palomuurin hallintaan.

Palveluverkkoa varten luodaan toinen sääntö, jotta sen sisäiset yhteydet toimivat ja koneet pääsevät internetiin. Vyöhykkeestä LAN-vyöhykkeeseen any (excluding Zywall) sallitaan palveluverkon IP-osoitteet. Tällä asetuksella palveluverkon koneet pystyvät liikennöimään myös toistensa kanssa. Tässäkin laitetaan lokitoiminto päälle.

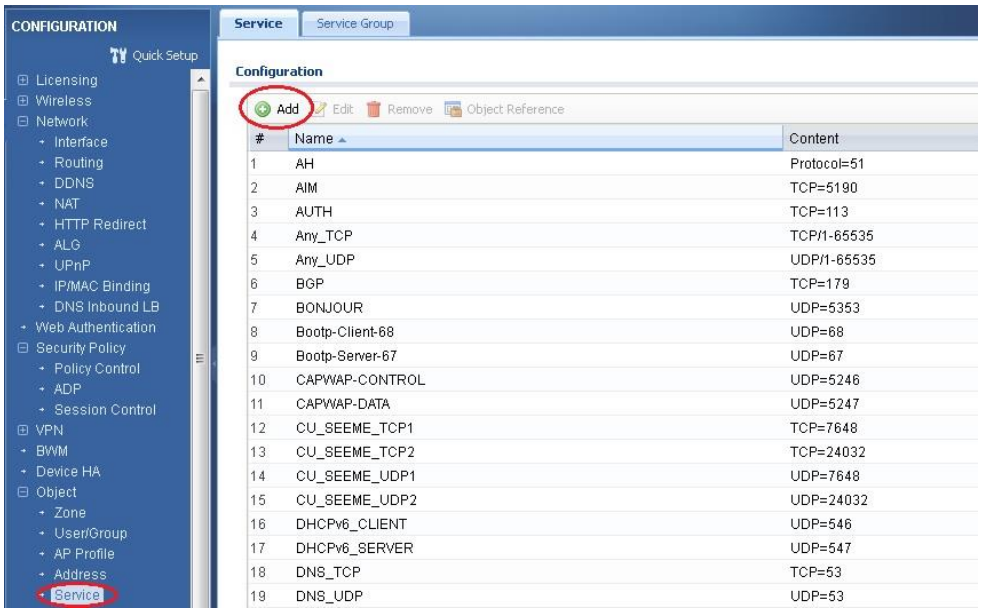
Asiakas-VLAN-verkoista liikenne ohjataan internetiin. Kuvassa 33 näkyvät vyöhykkeet, jossa VlanZone-vyöhykkeestä sallitaan liikenne WAN-liitäntään. Lähde- ja kohdeportte- ja sekä protokollia ei rajoiteta, koska tällä yhdellä säännöllä voidaan hallita kaikkia virtuaalilähiverkkoja.



Kuva 33. VLAN-verkkojen palomuurisääntö.

VPN-yhteyksiä varten luodaan ryhmä protokollista, joita tarvitaan yhteyden muodostamisessa. Yhteyttä varten olevat protokollat löytyvät valmiina palomuurin asetuksista. Ryhmään lisätään protokollat ESP, IKE ja NATT. IKE käyttää UDP:tä portilla 500 ja NATT UDP:tä portilla 4500. ESP:llä on käytössä portti 50. Ryhmien hallintaan pääsee Service-osiosta Service Group -välilehden kautta (kuva 34). NATT (aiemmin mainittu NAT Traversal) otetaan käyttöön, jotta VPN-yhteydet toimivat saman julkisen IP-osoitteen kautta.

Protokollia ja portteja lisätään kuvan 34 mukaisesti. Kuvassa näkyy myös joitakin jo valmiiksi laitettuja yleisimpiä portteja esim. AH ja BGP. Nämä ovat palomuurin sisäänrakennettuja asetuksia.



Kuva 34. Protokollan lisääminen objektiksi.

Asiakas-VPN-yhteyksissä verkon liikenne tulee palomuurista katsottuna IPSec-vyöhykkeestä. Tämä liikenne sallitaan LAN-vyöhykkeeseen. Lähdeporttina on etäyhteysverkon osoiteavaruus 170.10.10.0/24 ja kohdeosoitteena palveluverkko 192.168.10.0/24. Kaikki protokollat sallitaan. Koska yhteyksillä yleensä ylläpidetään palveluita SSH:lla ja HTTP:llä ja lisäksi käytetään tiedonsiirtoa, voitaisiin tässä rajoittaa liikenne vain näihin protokolliin.

Palomuurien välillä oleva site-to-site-VPN-tunnelin liikenne sallitaan samalla tavalla kuin asiakas-VPN-yhteyksissä. IPSec-vyöhykkeestä sallitaan liikenne AsiakasZone-vyöhykkeeseen, jossa lähdeosoitteena on asiakkaan oman palomuurin takana oleva verkko ja kohdeosoitteena yrityksen palomuurin takana oleva lähiverkko, jossa etähallittava palvelin sijaitsee. Yrityksen lähiverkon osoiteavaruus on 192.168.59.0/24. Kaikki protokollat sallitaan, koska ei tiedetä, minkälaista liikennettä VPN-tunnelissa kulkee.

Site-to-Site-tunnelia varten laitteen osoite 192.168.59.10 reititetään Policy-reitityksellä vastaanottavaan verkkoon. Next hop -osoitteeksi laitetaan asiakkaalle menevä IPSec-tunneli.

Palvelut, jotka osoitemuunnoksessa muutetaan sisäverkon IP-osoitteiksi, päästetään eteenpäin kohdeosoitteisiinsa. Näiden kaikkien palveluiden säännöt toteutetaan samal-

la tavalla. Kaikki yhteydet hyväksytään LAN-vyöhykkeeseen mistä tahansa IP-osoitteesta. Tulevaa osoitetta ei voi tarkemmin määrittää, koska yhteysyritykset tulevat internetin osoitteista ja sisäverkosta. Vastaanottavan osoite on laite, johon yhteys täytyy sallia. Jokaisella laitteella on oma julkinen IP-osoitteensa.

Taulukossa 3 näkyvät palveluiden nimi, vastaanottava portti ja protokollat, jotka sallitaan yhteyden luomisessa. Taulukossa 4 on tarkennettu protokollien yhteystyypit ja portit.

Taulukko 3. Palveluiden nimet, osoitteet ja protokollat.

Palvelun nimi	Vastaanottajan osoite	Protokollat
Web-hallintapaneeli1	192.168.10.58	dns-tcp, dns-udp, http, https, imap4, imap4s, Icewarp-smtp2, Icewarp-smtp, Mysql, pop3, pop3s, Hallintapaneeli, Hallintapaneeli-päivitys, Private-https-login, smtp
Exchange-palvelin	192.168.10.20	https, imap4, imap4s, pop3, pop3s, smtp, smtps, ssh-login-tcp, ssh-login-udp
Sähköpostipalvelin1	192.168.10.10	ftp, http, https, imap4, imap4s, IcewarpGroupware, Icewarp-IM, Icewarp-smtp2, Icewarp-smtp, pop3, pop3s, smtp, smtps
Backup-palvelin	192.168.10.72	ftp,http, privatehttps-login
Dns-palvelin 1	192.168.10.15	dns-tcp, dns-udp

Taulukko 4. Taulukon 3. protokollien yhteystyypit ja porttinumerot tarkemmin.

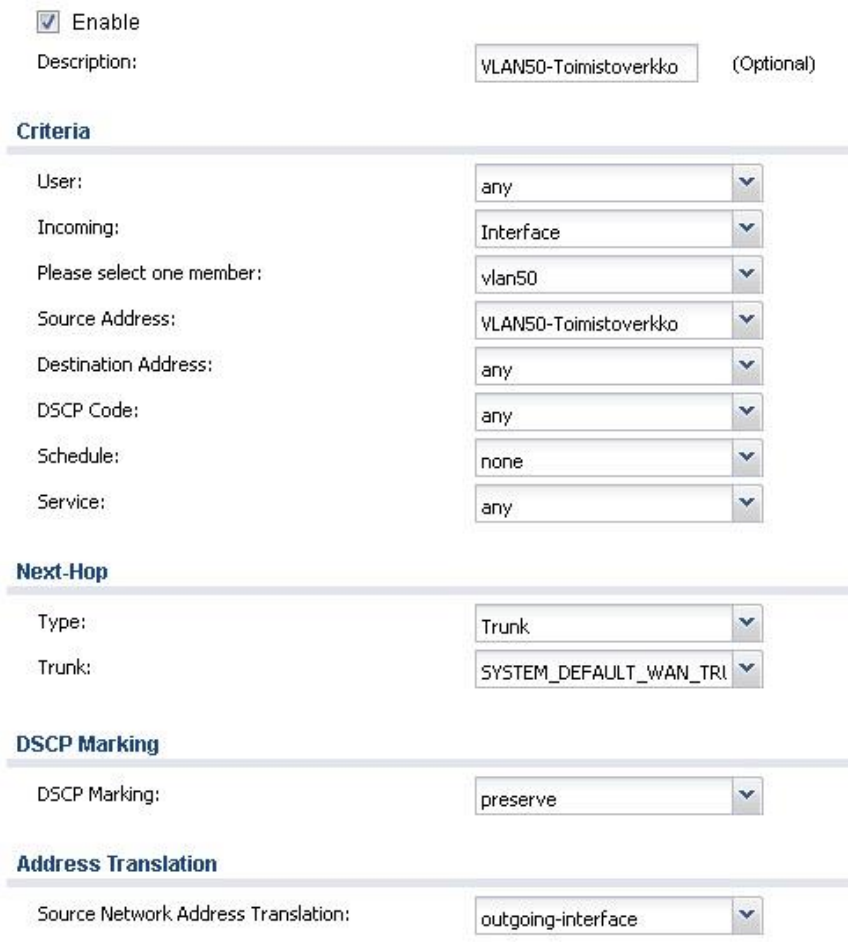
Protokolla	Yhteystyyppi	Porttinumero tai -numerot
ftp	tcp	20-21
http	tcp	80
https	tcp	143
imap4	tcp	143
imap4s	tcp	993
IcewarpGroupware	tcp	5229
Icewar-IM	tcp	5222-5223
Icewarp-smtp2	tcp	587
Icewarp-smtp	tcp	366
pop3	tcp	110
pop3s	tcp	995
Hallintapaneeli	tcp	8800
Hallintapaneeli-päivitys	tcp	8447
Private-https-login	tcp	8080
ssh-login-tcp	tcp	22
ssh-login-udp	udp	22

Koska yhteysyritykset on sallittu kaikista julkisista osoitteista sisäverkkoon, on tärkeää rajoittaa liikenne vain sellaisiin protokolliin, joita yhteydessä tarvitaan. Tulevissa yhteyksissä käytetään protokollatyypille tyypillisiä porttinumeroita, jotta useimmat laitteet osaavat suoraan liikennöidä oikealla tavalla yrityksen palveluihin. Yhteyksiin voisi saada lisäturvaa tekemällä porttiohjauksia sisäiseen verkkoon ja käyttämällä vähemmän tunnettujen palveluiden kanssa joitain muita porttinumeroita. Porttiohjauksesta esimerkkinä voisi olla HTTP-yhteys, jossa tuleva liikenne ohjattaisiin portista 80 porttiin 8080. Taulukossa 4 on esimerkki Icewarp-smtp-protokollasta, joka käyttää oletusportin 25 sijasta porttia 366.

3.9 Reitityssäännöt

Palomuurissa reititykset tehdään Policy-based routing (PRB) -menetelmällä. Nämä reitit toteutetaan silloin, kun suoraa reittiä ei ole. Virtuaalilähiverkkojen reititykselle tehdään omat säännöt.

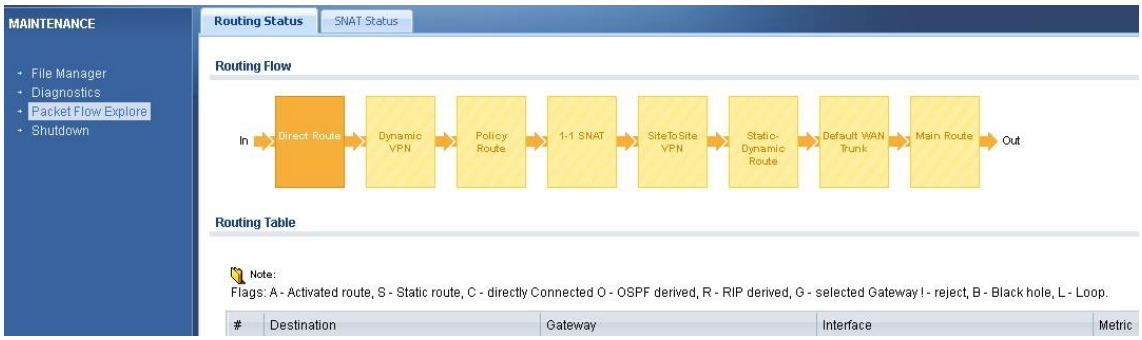
Virtuaalista toimistoverkkoa varten luodaan oma reitityssääntö kuvan 35 mukaisesti. Tulevaksi liitännäksi valitaan Toimistoverkon VLAN 50 -liitäntä sen omalla IP-osoitealueella. Liikenne reititetään ulospäin WAN Trunk -liitäntään. Tuleviin yhteyksiin täytyy tehdä staattinen osoitemuunnos, jossa verkon sisäinen osoite muutetaan julkiseksi. Muille virtuaalilähiverkoille tehdään samanlaiset reitityssäännöt kuin Toimistoverkolle. Lähdeosoitteena käytetään virtuaaliverkon omaa IP-osoitealuetta.



Kuva 35. Policy-based routing -säännön tekemien VLAN-toimistoverkkoon.

IPSec-tunnelilla toteutettua varmuuskopiointia varten liikenne reititetään suoraan sen VPN-tunneliin (Next hop). Lähdeosoitteena voivat olla verkon 192.168.10.0/24 osoitteet ja vastaanottavana varmuuskopiointiverkon IP-osoitealue 192.168.45.0/24.

Verkkojen reititystiedot voidaan katsoa palomuurin hallinnasta kohdasta Packet flow explore ja välilehdestä Routing status (kuva 36).



Kuva 36. Routing status -näkymä, josta voi tarkastaa olemassa olevat reititykset.

Kuva 36 näyttää, missä järjestyksessä verkkoja reititetään. Ensin toteutetaan suorat reitit ja sen jälkeen Policy Routella tehdyt jne.

4 Palomuurin ylläpito, testaus ja liikenteen seuraaminen

Palomuurivaihdon jälkeen käynnistetään kaikki kytkimet uudelleen, jotta niiden ARP-taulut saadaan tyhjennettyä nopeasti ja voidaan huomata, että liikenne toimii. Vaihdon jälkeen tarkastetaan palveluiden ja internetyhteyden toimivuus. Kaikki sisäverkon laitteet vastaavat Ping-kyselyyn, joten sisäverkko voidaan todeta toimivaksi. DHCP-taulussa näyttää olevan oikein jaettuja osoitteita Toimisto- ja virtuaalilähiverkoille.

Ongelmia pystytään havaitsemaan tutkimalla palomuurin lokia jatkuvasti. Lokiin kerätään tietoja yhteysyrityksistä ja yritetään etsiä estetty liikenne. Havaitaan, että Exchange-sähköpostipalvelin ei toimi halutulla tavalla. Laite vastaa Ping-kyselyyn, mutta se ei pysty liikennöimään internetiin. Osoitemuunnoksessa on väärä julkinen IP-osoite, ja tämä saadaan toimivaksi vaihtamalla se oikeaksi.

Yrityksen ja asiakkaan välisessä IPSec-menetelmässä huomataan myös ongelma. Palomuurien välillä näyttää olevan jonkinlainen yhteys, mutta mitään liikennettä siinä ei kulje. Havaitaan, että asiakkaan palomuurin vaihe 2 –asetuksissa on väärä salaustyyppi. Tämä vaihdetaan AES128:ksi. Lisäksi toisen laitteen sisäverkkoon ei kulje liikennettä, joten sen kohdalla joudutaan muuttamaan palomuurisääntöä. Palomuurisäännössä on asetettu väärä asiakaspään verkko. Tämä korjataan oikeaksi.

Kuvassa 37 näkyy IPSec-tunnelin luomisessa käytettäviä menetelmiä. Siinä hyväksytään SA-sopimus (SA), käytetään Diffie Hellmanin algoritmia (HASH) ja vaihdetaan vertaisten väliset ID-numerot (ID). Yhteyden elinikä hyväksytään (LIFETIME) ja salataan ESP-protokollalla. Kun SA-sopimukset hyväksytään ja yhteys salataan, tunneli on valmis.

	Pri...	Cat...	Message	Source	Destination	Note
06:38:08	info	IKE	Tunnel [Backup Backup 0xb08af0e4] built successfully	500	500	IKE_LOG
06:38:08	info	IKE	[ESP des-cbc|hmac-sha1-96][SPI 0xe5fe3ea6|0xb08af0e4][Lifetim...	500	500	IKE_LOG
06:38:08	info	IKE	[Policy: ipv4(192.168 192.168. -ipv4(.	500	500	IKE_LOG
06:38:08	info	IKE	[Initiator:][Responder:	500	500	IKE_LOG
06:38:08	info	IKE	Send:[HASH]	500	500	IKE_LOG
06:38:08	info	IKE	Recv:[HASH][SA][NONCE][ID][ID][NOTIFY:RESPONDER_LIFETIME]	500	500	IKE_LOG
06:38:08	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	500	500	IKE_LOG
06:38:08	info	IKE	Send:[HASH][DEL] [count=3]	500	500	IKE_LOG

Kuva 37. IPSec-tunnelin neuvottelua.

Muut VPN-yhteydet ovat yhdistyneet normaalisti ja palomuurissa näkyy IKE-yhteyksiä ja neuvoteltuja SA-sopimuksia.

Nimipalvelupyyntöjä alkaa tulla normaalisti. Niitä pystyy tutkimaan tarkemmin Session monitor -välilehdellä (kuva 38.). Kyselyt ohjataan oikeaan sisäverkon IP-osoitteeseen ja porttiin 53.

Session Monitor

admin (13 Sessions)

				1.01 MBytes	45.30 KBytes
- (37 Sessions)					
	DNS_UDP	182.254. 39781	53	56 Bytes	56 Bytes
	DNS_UDP	193.65. :50343	53	63 Bytes	63 Bytes
	DNS_UDP	62.148. 49797	53	74 Bytes	74 Bytes
	DNS_UDP	62.148. :5230	53	74 Bytes	74 Bytes
	HTTP	91.159. 28371	80	112 Bytes	538 Bytes
	HTTPS	109.240. :49855	443	3.554 KBytes	1.465 KBytes
	DNS_UDP	208.69. 5406	53	180 Bytes	89 Bytes
	DNS_UDP	134.170. :59364	53	169 Bytes	76 Bytes
	DNS_UDP	62.148. :21153	53	71 Bytes	71 Bytes
	DNS_UDP	83.145. :45282	53	184 Bytes	74 Bytes
	DNS_UDP	195.197. :62299	53	145 Bytes	61 Bytes

Kuva 38. Session monitor -näkymä, jossa näkyy avoinna olevat yhteydet.

Kuvassa 38. DNS-kyselyt tulevat julkisista IP-osoitteista yrityksen julkiseen osoitteeseen. Ensimmäinen sarake, jossa näkyy tiedonsiirron määrä, tarkoittaa vastaanotettuja paketteja. Viimeinen sarake osoittaa lähetettyjen pakettien määrän.

Sähköpostipostipalvelut lähtivät toimimaan normaalisti. Yhteysyrityksiä tuli esimerkiksi portteihin 110 ja 993. Sähköpostin vastaanotto ja lähetys testattiin myös käytännössä omalla sähköpostilla.

Virtuaalilähiverkkojen testaus suoritettiin kerroskytkimestä. Kytkin jakoi oikeaa verkkoa oikeista porteista. Internetiin pääsy toimi moitteettomasti, ja verkoissa olevat laitteet vastasivat Ping-kyselyihin. VLAN:en välillä yhteysyritykset estettiin.

Resurssien käyttöä valvotaan palomuurista jatkuvasti, mutta valvontaan kiinnitetään erityisesti huomiota parin päivän aikana palomuurivaihdosta. Laitteen prosessorikuorma on maksimissaan noin 20 %:n luokkaa ja muistia käytetään vain noin 30 % maksimista. Lukemat kertovat, että laite selviytyy hyvin tehtävästään ja pystyy toistaiseksi toimimaan hyvin pienellä kuormituksella. Tämän jälkeen laitteen valvontaa jatketaan normaalisti. Yhteysyrityksiä seulotaan ja palomuurin läpi menevää liikennettä tarkkaillaan.

5 Yhteenveto

Tässä opinnäytetyössä käsitellään palomuurivaihtoon liittyviä ominaisuuksia, protokollia ja niiden toimivuutta. Näiden avulla pystytään suunnittelemaan ja rakentamaan palomuuri, joka vastaa yrityksen tarpeita. Tarkempi perehtyminen esimerkiksi palomuurin suodatusmenetelmiin ja VPN-verkkoihin auttaa ymmärtämään niiden toimivuutta ja tarkoitusta tässä kontekstissa.

Opinnäytetyö on haastava ja siihen paneutuminen vie paljon aikaa. Huomaan, että eri laitevalmistajat käyttävät samasta asiasta eri termejä ja tämä vaikeuttaa erityisesti tiedon hankintaa. Tietoa täytyy hakea useammasta lähteestä ja sitä pitää pyrkiä referoimaan tarkasti teoriaosuudessa.

Tarkan suunnitelman laatiminen työn vaiheista ja asennuksesta helpottaa asennuksen toteutusta ja auttaa ongelmien ilmetessä. Erityisesti palomuurisääntöjen kanssa joutuu olemaan tarkkana, että haluttu liikenne pääsee läpi palomuurista. Näitä joutuukin säätämään ja miettimään uudelleen useamman kerran.

Vaihtotyö on onnistunut pääpiirteissään, sillä kaikki ongelmat on saatu ratkaistua nopeasti. Lisäksi palomuuriasetukset on saatu dokumentoitua ja niiden osia voidaan kuvata tai liittää tietoturvasuunnitelmaan. Laitteesta saadaan varmuuskopioitua asetustiedosto ja asetukset voidaan tarvittaessa palauttaa. Työtä voisi parantaa määrittämällä palomuurisäännöt tarkemmin mahdollisen haitallisen liikenteen takia. Säännöt tulisi kartoittaa tarkasti ja dokumentoida sallittu liikenne.

Tulevaisuudessa asiakasmäärät kasvavat etenkin sähköpostipalveluiden osalta. On oletettavaa, että palomuurin taakse rakennettavat virtuaalipalvelimet ja niin kutsutut pilvipalvelut yleistyvät. Niiden toiminta on tärkeää turvata jatkossa.

Lähteet

1. Morris-mato. Verkkodokumentti. http://fi.wikipedia.org/wiki/Morris-mato. Luettu 15.1.2015

2. Windowsin palomuurin käyttäminen. Verkkodokumentti. http://windows.microsoft.com/fi-fi/windows-xp/help/networking/using-windows-firewall. Luettu 15.1.2015.

3. OS X: Tietoa sovelluspalomuurista. Verkkodokumentti. http://support.apple.com/fi-fi/HT1810. Luettu 15.1.2015.

4. Hakala Mika, Vainio Mika, Vuorinen Olli. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

5. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

6. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Kuva 3-3. Helsinki: Edita Publishing Oy.

7. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

8. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

9. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Kuva 3-5. Helsinki: Edita Publishing Oy.

10. Palomuuritekniikoita. Verkkodokumentti. http://www.okol.org/verkkokurssit/datanomi/tietojarjestelmien_kehittaminen/tietoturvajarjestelmat/palomuurit/palomuuritekniikoita.htm. Luettu 24.1.2015

11. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

12. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

13. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

14. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

15. Hakala Mika, Vainio Mika, Vuorinen Olli. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

16. Hakala Mika, Vainio Mika, Vuorinen Olli. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

17. VLAN-merkintä. Verkkodokumentti. http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanmerkint.html. Luettu 15.3.2015.

18. VLAN-merkintä. Verkkodokumentti. http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanmerkint.html. Luettu 15.3.2015.

19. Hakala Mika, Vainio Mika, Vuorinen Olli. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

20. Hakala Mika, Vainio Mika, Vuorinen Olli. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

21. Hakala Mika, Vainio Mika, Vuorinen Olli. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

22. VLAN-perusteet. Verkkodokumentti. http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanperusteet.html. Luettu 12.3.2015.

23. Vahti. Tietojärjestelmiin kohdistuvat vaatimukset. Verkkodokumentti. https://www.vahtiohje.fi/web/guest/tietojarjestelmiin-kohdistuvat-vaatimuk-set;jsessionid=815C6581B532A8EAF74D5EBBFBD88D659221345A4EB46D1CEA4CB6EF72A17D253C3A3E245B74AB6D6E57A8?p_p_id=56_INSTANCE_G74d&p_p_lifecycle=0&p_p_state=exclusive&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_56_INSTANCE_G74d_struts_action=%2Fjournal_content%2Fview&_56_INSTANCE_G74d_groupId=10128&_56_INSTANCE_G74d_articleId=29355&_56_INSTANCE_G74d_viewMode=print. Luettu 15.3.2015.

24. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

25. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

26. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

27. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

28. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

29. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

30. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

31. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

32. Mason Andrew. 2002. IPSec overview part four: Internet key exchange (IKE). Verkkodokumentti. Luettu 20.3.2015.

33. Mmitesha. 2009. Verkkodokumentti. https://supportforums.cisco.com/document/31741/main-mode-vs-aggressive-mode. Luettu 22.3.2015.

34. IPsec made simple. Verkkodokumentti. https://briolidz.wordpress.com/2012/01/23/ipsec-made-simple/. Luettu 28.3.2015.

35. Thomas Tom. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Publishing Oy.

36. Zywall 1100/310/110. Verkkodokumentti. http://www.zyxel.com/fi/fi/products_services/zywall_1100_310_110.shtml?t=p&utm_source=NL1308_FI_promo3&utm_medium=email&utm_campaign=NL1308_FI_promo3_L_IMG-B_2-4_@HELLO_FI. Luettu 28.3.2015.

37. Difference between IKEv1 and IKEv2. Verkkodokumentti. http://www.differencebetween.net/technology/protocols-formats/difference-between-ikev1-and-ikev2/. Luettu 10.4.2015.

38. Jim. 2014. What is IPsec NAT-Traversal?? Verkkodokumentti. http://thejimmahknows.com/nat-traversal-ipsec/. Luettu 10.4.2015.

39. Zywall 110/310/1100 Series VPN. Verkkodokumentti. ftp://ftp.zyxel.com/ZyWALL_310/user_guide/ZyWALL%20310_V3.10_Ed2.pdf. Luettu 18.1.2015.

Suunnitelma palomuurivaihdon toteutuksesta

Toimenpiteet ja aikataulu

Palomuurin vaihtaminen toteutetaan kevään 2015 aikana. Työ käynnistetään tammikuussa ja huuhtikuussa työn tulisi olla valmis. Aikataulusuunnitelma on seuraava:

- tammikuu – helmikuu 2015
    - Kerätään tietoa palomuurin toiminnasta ja siihen liittyvistä asioista.
    - Tehdään suunnitelma palomuuriasetuksista
- maaliskuu 2015
    - Valmistellaan palomuuri asetuksien määrittämistä varten.
    - Toteutetaan asennus niin pitkälle kuin mahdollista.
    - Tarkastellaan ilmeneviä ongelmia ja arvioidaan, tulisiko jotain muuttaa
- Huuhtikuu 2015
    - Viimeistellään asennus ja testataan palomuuria
    - Dokumentoidaan palomuurin toiminta ja sen periaate
    - Asiakkaille lähetetään tietoa vaihtotyöstä viikkoa ennen työn aloittamista
    - Otetaan varmuuskopio laiteasetuksista ennen vaihtotyötä
    - Toteutetaan palomuurivaihto

- Testataan VPN-yhteydet, verkkojen, palveluiden ja varmuuskopioinnin toimivuus

- Arvioidaan työn onnistumista ja muutetaan asetuksia, jos jokin menee vikaan

- Varmuuskopioidaan palomuurista viimeisin laiteasetus, kun tilanne on stabiloitunut.

Uuden palomuurin asetuksien suunnittelu ja laittaminen vaativat eniten aikaa tässä työssä ja niihin panostetaan ajallisesti eniten. Asetuksien määrittäminen on monimutkainen toimenpide, jota pyritään kehittämään samalla, kun työtä tehdään. Tämä voi hidastaa työn asennusvaihetta. Asennusta varten kerätään mahdollisimman paljon tietoa käytettävistä protokollista, nykyisistä verkoista, salauksista, salasanoista jne.

Palomuurin vaihtaminen vaikuttaa asiakkaiden ja oman henkilökunnan toimintaan ja työhön. Huoltotyöstä lähetetään sähköposti-ilmoitus asiakkaille viikkoa ennen työn aloitusta. Vaihtotyö tehdään ilta-aikaan, jolloin siitä on mahdollisimman vähän haittaa. Katkos arvioidaan olevan noin 6-7 minuuttia, jonka jälkeen palvelut pyritään saamaan toimintaan mahdollisimman nopeasti. Vaihtotyön aikaikkunaksi on asetettu 4 tuntia.

Palveluiden ja liikenteen kartoitus

Palomuurivaihdon yhteydessä luodaan uusia lähi-, VLAN- ja VPN-verkkoja. Vanhoja verkkoja – kuten palveluverkko ja asiakkaiden virtuaalilähiverkkoja – ei muuteta. Näiden asetukset laitetaan palomuuriin samanlaisina kuin aiemmin.

Palveluita pyritään toteuttamaan laadukkaasti. Asiakkaat tarvitsevat nopean, turvallisen ja varman pääsyn palveluihin vuorokauden ympäri. Palveluiden käyttö tarvitsee tehokkaan palomuurin ja varsinkin VPN-liikenteen salaamisessa ja purkamisessa yhteys tulisi toimia moitteettomasti ja nopeasti.

Pääsynhallinta

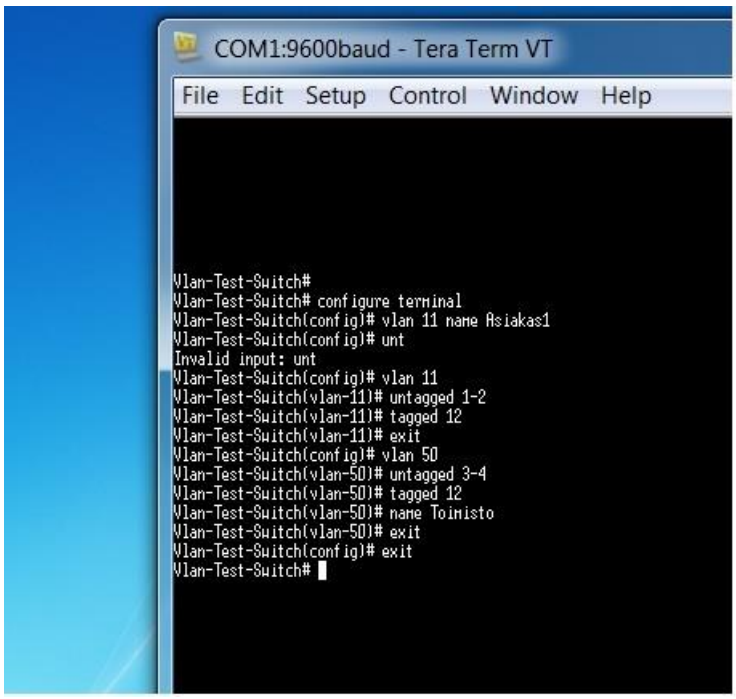
Palomuurin pääsy toteutetaan siten, että ainoastaan yrityksen omasta palveluverkosta pääsee kirjautumaan siihen. Kirjautumisessa käytetään HTTPS-yhteyttä ja yksityistä porttia.

Käyttäjätunnuksena kirjautumiseen käytetään tiettyä admin-tunnusta, jolla on oikeudet tehdä muutoksia palomuuriin. Tarvittaessa käytetään limited-admin:ia, jolla pystytään tarkastelemaan palomuurin asetuksia, mutta ei tekemään siihen muutoksia. User-tason oikeuksilla toteutetaan palveluiden käyttäjätodennus. Taulukossa 5. on esitetty Zywall 310 –laitteen kirjautumistyypit.

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change ZyWALL configuration (web, CLI)	WWW, TELNET, SSH, FTP, Console
limited-admin	Look at ZyWALL configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH, Console
Access Users		
user	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
guest	Access network services	WWW
ext-user	External user account	WWW
ext-group-user	External group user account	WWW

Taulukko 5. Zyxel Zywall 310 -käyttäjätyypit [39, s. 3.]

VLAN-verkkojen testaukset



Samassa VLAN-verkossa olevien laitteiden liikenteen testaus.

PC1-asetukset.

```
Ethernet-sovitin Lähiverkkoyhteys:

      Yhteyskohtainen DNS-liite . . . . : fixcom.fi
   Linkin paikallinen IPv6-osoite. . : fe80::c92c:cb16:80c1:23cc%11
   IPv4-osoite . . . . . . . . . . . : 180.80.10.10
      Aliverkon peite . . . . . . . . : 255.255.255.0
      Oletusyhdyskäytävä. . . . . . . : 192.168.2.10
                                        180.80.10.254
```

PC2-asetukset.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : fixcom.fi
   Link-local IPv6 Address . . . . . : fe80::9c6c:ea02:e622:1fb8%10
   IPv4 Address. . . . . . . . . . . : 180.80.10.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 180.80.10.254
```

Ping-testi koneesta PC1 koneeseen PC2.

```
C:\Users\Järjestelmänvalvoja>ping 192.168.50.20

Ping-isäntä: 192.168.50.20 32 tavua tietoja:
Pyyntö aikakatkaistiin.
Pyyntö aikakatkaistiin.
Pyyntö aikakatkaistiin.
Pyyntö aikakatkaistiin.

Ping-tilastot 192.168.50.20:
    Paketit: Lähetetty = 4, Vastaanotettu = 0, Kadonnut = 4
             (100% hävikki),
```

Eri VLAN-verkossa olevien laitteiden liikenteen testaus

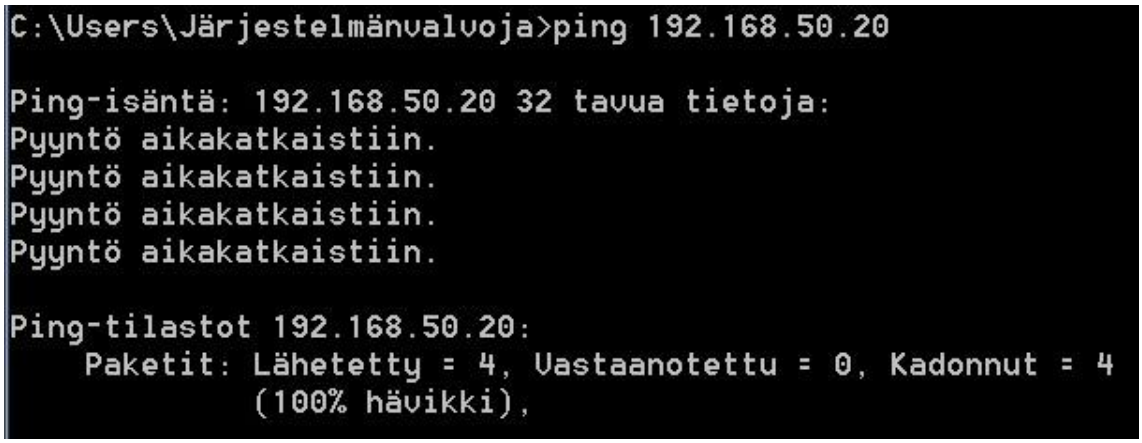
PC1-asetukset.

```
Ethernet-sovitin Lähiverkkoyhteys:

       Yhteyskohtainen DNS-liite . . . . : fixcom.fi
   Linkin paikallinen IPv6-osoite. . : fe80::c92c:cb16:80c1:23cc%11
   IPv4-osoite . . . . . . . . . . . : 180.80.10.10
       Aliverkon peite . . . . . . . . . : 255.255.255.0
       Oletusyhdyskäytävä. . . . . . . . : 192.168.2.10
                                           180.80.10.254
```

PC2-asetukset.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : fixcom.fi
   Link-local IPv6 Address . . . . . : fe80::9c6c:ea02:e622:1fb8%10
   IPv4 Address. . . . . . . . . . . : 192.168.50.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.254
```

Ping-testi koneesta PC1 koneeseen PC2.



VLAN-testikytkimen asetukset

Running configuration:

; J4812A Configuration Editor; Created on release #F.05.22

hostname "Vlan-Test-Switch"
cdp run
snmp-server community "public" Unrestricted
vlan 1
name "DEFAULT_VLAN"
untagged 5-14
ip address dhcp-bootp
no untagged 1-4
exit
vlan 11
name "Asiakas1"
untagged 1-2
tagged 12
exit
vlan 50

```
   name "Toimisto"
   untagged 3-4
   tagged 12
   exit
no aaa port-access authenticator active
```

Shrew Softin Access Manager –ohjelman VPN-asiakasasetukset

n:version:4
n:network-ike-port:500
n:network-mtu-size:1380
n:client-addr-auto:0
n:network-natt-port:4500
n:network-natt-rate:15
n:network-frag-size:540
n:network-dpd-enable:1
n:client-banner-enable:0
n:network-notify-enable:1
n:client-dns-used:0
n:client-dns-auto:0
n:client-dns-suffix-auto:0
n:client-splitdns-used:0
n:client-splitdns-auto:0
n:client-wins-used:0
n:client-wins-auto:0
n:phase1-dhgroup:2
n:phase1-life-secs:3600
n:phase1-life-kbytes:0
n:vendor-chkpt-enable:0
n:phase2-life-secs:3600
n:phase2-life-kbytes:0
n:policy-nailed:0
n:policy-list-auto:0
n:phase1-keylen:128
n:phase2-keylen:128
s:network-host:193.229.108.59
s:client-auto-mode:disabled
s:client-iface:virtual
s:client-ip-addr:10.10.15.1
s:client-ip-mask:255.255.255.0
s:network-natt-mode:enable

s:network-frag-mode:enable
s:auth-method:mutual-psk-xauth
s:ident-client-type:address
s:ident-server-type:address
s:ident-client-data:20.30.1.10
s:ident-server-data:10.10.15.254
b:auth-mutual-psk:dDQzI2dsLWxrIUptcmJlZ3o5b1ZzZGZyYjlpMFllc3Y=
s:phase1-exchange:main
s:phase1-cipher:aes
s:phase1-hash:sha2-256
s:phase2-transform:esp-aes
s:phase2-hmac:sha2-256
s:ipcomp-transform:disabled
n:phase2-pfsgroup:2
s:policy-level:unique
s:policy-list-include:192.168.50.0 / 255.255.255.0
s:client-saved-username:Testi